A STUDY ON DATABASE MARKETING PRACTICES THAT RAISE CONSUMER PRIVACY CONCERN: A PROPOSED MODEL FOR REGULATING DATABASE MARKETING PRACTICES IN SOUTH AFRICA

BY

DIANE VISSER

ASSIGNMENT PRESENTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTERS OF COMMERCE
(BUSINESS MANAGEMENT)
AT THE UNIVERSITY OF STELLENBOSCH

SUPERVISOR: PROFESSOR N S TERBLANCHÉ

DECEMBER 2002
STELLENBOSCH

DECLARATION

I, the undersigned, hereby declare that the work contained in this assignment is my own original work and has not previously in its entirety or in part been submitted at any university for a degree.

Diane Visser

ABSTRACT

One of the phenomena's in the marketing industry of the past decade is the increased use of database marketing. Database marketing involves the collection, processing and dissemination of vast amounts of consumer information in order to compile detailed consumer databases. The increasing popularity of database marketing can be attributed to various factors. Consumer information can now be obtained easier, cheaper and faster due to the availability of information technology. It has become easier to segment consumer markets and it is possible to identify consumer trends. It is possible to make predictions of consumer behaviour or buying patterns because consumer databases provide a more complete consumer profile with information ranging from demographics, psychographics to life-style information. Database technology improves the efficiency and effectiveness of marketing campaigns because marketers can analyse the available information and select the most appropriate marketing strategies and tactics, while concentrating efforts on the most profitable consumer. Marketers therefore waste less effort, money, and other resources by not promoting to individuals who are unlikely to react upon such offers. Widespread databases assist marketers in offering products that are more reasonably priced and more precisely tailored for smaller, more homogeneous market segments. Improved product and service offerings as well as the availability of a wider variety of products and services will likely result in higher consumer satisfaction and could build consumer loyalty. Therefore, marketers use consumer information to improve the overall marketing strategy and individual customer service.

Consumers are concerned about database marketing practices because consumers believe some data practices invade personal privacy. The need for privacy has always been inherent to human nature and the concept of privacy dates back to early mankind. One should however differentiate between an individual's basic need for privacy from a general perspective and privacy within a consumer-marketer context. Privacy from a general perspective refers to one's territoriality and need for physical seclusion, whereas consumer privacy mainly relate to the privacy of personal information. Bennett, as well as Stone and Stone proposed that a state of privacy exist when a consumer can control social interaction, unwanted external stimuli, and the dissemination of personal information as well as being able to make independent decisions without outside interference. Consumers' need for privacy is however, in conflict with the need for social interaction and the need to participate in commercial exchange relationships. The more a person interacts with other members of

society, the more the person could expect to compromise some privacy. This implies that when consumers participate in a business transaction, or where an exchange relationship exists between the database marketer and consumer, consumers could expect that a degree of privacy will be lost.

Consumer groups however, argue that some marketing practices invade the reasonable amount of privacy consumers should be able to expect. The raising consumer concern for privacy is attributable to several reasons. The primary driver of consumer concern is the general lack of knowledge on data collection and use. Other reasons for the raising privacy concern include the type of information collected and the amount of control consumers have over subsequent use of data; the use of personal information to identify specific individuals; collection and use of sensitive information, such as medical and financial data; the volume of information collected and used; secondary information use; the use and dissemination of inaccurate databases; the collection and use of children's data; the lack of tangible benefits received in exchange for information provided; and the use of consumer information for financial gain. Consumers have also expressed concern about electronic database marketing practices because of the secrecy in data collection and use. However, privacy concerns may vary depending on consumers' cultural orientation, age, perception on what constitutes good marketing ethics or the specific methods employed to obtain consumer data. One could distinguish between several consumer clusters when considering consumers' attitudes on database marketing practices and personal privacy. In this regard the typical South African consumer is classified as a "pragmatist". Pragmatists are concerned with privacy to the extent they are exposed to database marketing activities. The South African database marketing industry is still in its infancy phase and as the industry progress, and consumers become more knowledgeable, privacy concerns are likely to increase.

It is important to address the issues that raise consumer privacy concerns and to find solutions for ensuring sustainable database marketing practice in future. Marketers' information needs and consumers' privacy needs should somehow be balanced in order to withhold government intervention. Compromises from both sides are necessary to reach a more balanced relationship between the two parties. The successful outcome of the privacy debate will depend on marketers' understanding of consumer privacy issues and by addressing these accordingly.

Several approaches exist for regulating database marketing practices that invade consumer privacy: the implementation of information technology, self-regulation and government intervention. Self-regulation is preferred for regulating database marketing practices, whereas privacy-enhancing information technology is recommended as a supplemental tool for protecting consumer privacy. Government regulating seems to be the last resort because of unnecessary restrictions that might be imposed on database marketing activities.

Recommended models for regulating database marketing activities and for protecting consumer privacy in South Africa are the Registration Model, together with elements of the Data Commissioner Model. These models were proposed after careful consideration of characteristics, unique to the South African database marketing industry. The models place the responsibility for data protection with the database marketer and the South African government, rather than with the consumer. The Registration Model and the Data Commissioner Model seems a viable combination for implementation in South Africa because these models acknowledge the fact that South African pragmatic consumers are not well educated and informed enough on privacy invading database marketing practices. This combination rarely involves any consumer participation and therefore suits the typical apathetic nature of South African consumers.

The Registration Model acts like a notice system where an agency, currently the Direct Marketing Association of South Africa, develops principles of fair information practices to which registered marketers need to comply with. A commission, an element of the Data Commissioner Model, has power to investigate consumer complaints, constrain development of databases, review data practices and advise on improvements on data collectors' systems. The commission could also monitor advancements in information technology that may enhance consumer privacy. The only problem with these models seems to be that the agency and or the commission have no authoritative power to enforce compliance with principles and codes of conduct.

Industry self-regulation in conjunction with some governmental control and the application of information technology seems to be useful in providing adequate levels of consumer privacy and data protection. Such a combination might strike a balance between South African consumers' need for privacy and South African marketers' need for consumer information.

OPSOMMING

Een van die verskynsels in die bemarkingsindustrie oor die afgelope dekade is die toenemende gebruik van databasisbemarking. Databasisbemarking behels die insameling, prosessering en verspreiding van groot hoeveelhede verbruikersinligting met die doel om gedetailleerde verbruikersdatabasisse saam te stel. Die toenemende gewildheid van databasisbemarking kan toegeskryf word aan verskeie faktore. Inligtingstegnologie maak dit baie makliker, goedkoper en vinniger om verbruikersinligting te bekom. Dit raak al hoe makliker om verbruikersmarkte te segmenteer en dit is moontlik om verbruikers tendense te identifiseer. Voorspellings kan ook gemaak word ten opsigte van verbruikersgedrag en aankooppatrone omdat die omvang van inligting in verbruikersdatabasisse strek vanaf demografiese, psigografiese tot lewenstylinligting en daarom 'n baie meer volledige verbruikersprofiel bied. Databasistegnologie verbeter die doeltreffendheid en effektiwiteit van bemarkingsveldtogte omdat bemarkers beskikbare inligting kan analiseer en die mees gepaste bemarkingstrategieë en taktieke kan selekteer, terwyl programme gerig kan word op die mees winsgewinde verbruiker. Bemarkers sal dus minder moeite, geld en ander hulpbronne vermors deurdat bemarkingsprogramme nie gerig word op individue wat heel waarskynlik nie op sulke aanbiedinge sal reageer nie. Omvangryke databasisse help bemarkers om goedkoper produkte te bied wat meer presies ontwerp is op kleiner, meer homogene marksegmente te dien. Verbeterde produk en diens aanbiedinge tesame met die beskikbaarheid van 'n wyer verskeidenheid van produkte en dienste, sal heel waarskynlik hoër verbruikersatisfaksie tot gevolg hê en kan verbruikerslojaliteit bewerkstellig. Dus, bemarkers gebruik verbruikersinligting om die algehele bemarkingstrategie en individuele diens aan verbruikers te verbeter.

Verbruikers het belang by databasis bemarkingspraktyke omdat verbruikers glo dat sommige data praktyke inbreuk maak op persoonlike privaatheid. Die behoefte aan privaatheid was nog altyd inherent aan die menslike natuur en die konsep van privaatheid dateer terug tot vroeë beskawings. Daar behoort egter 'n onderskeid getref te word tussen 'n individu se basiese behoefte aan privaatheid vanuit 'n algemene perspektief en privaatheid vanaf 'n verbruiker-bemarker konteks. Privaatheid, vanaf 'n algemene perspektief, verwys na 'n individu se persoonlike ruimte en die behoefte aan fisiese afsondering, teenoor verbruikersprivaatheid wat hoofsaaklik verband hou met die privaatheid van persoonlike inligting. Bennett, sowel as Stone en Stone het voorgestel dat 'n mate van privaatheid heers wanneer 'n verbruiker beheer het oor sosiale interaksies, ongewenste eksterne prikkels, die

verspreiding van persoonlike inligting, sowel as om in staat te wees om onafhanklike besluite te neem sonder invloed van buite. Verbruikers se behoefte aan privaatheid is egter in konflik met die behoefte aan sosiale interaksie en die behoefte om deel te neem aan kommersiële transaksies. Hoe meer 'n persoon in wisselwerking tree met ander lede van die gemeenskap, hoe meer kan die persoon verwag om 'n mate van privaatheid op te offer. Dit impliseer dat wanneer verbruikers deelneem in 'n besigheidstransaksie of waar 'n ruilverhouding bestaan tussen die databasisbemarker en verbruiker, kan verbruikers verwag dat 'n mate van privaatheid verlore sal gaan.

Verbruikers kan 'n redelike mate van privaatheid verwag, maar verbruikersgroepe argumenteer dat sommige bemarkingspraktyke inbreuk maak op hierdie redelike verwagting van privaatheid. Die toenemende verbruikersbelang by privaatheid is toeskryfbaar aan verskeie redes. Die primêre dryfkrag agter verbruikers se belang is die algemene gebrek aan kennis oor data insameling en gebruik. Ander redes wat bydrae tot die toenemende belang by privaatheid sluit in die tipe inligting ingesamel en die hoeveelheid beheer verbruikers het oor die daaropeenvolgende gebruik van data; die gebruik van persoonlike inligting om spesifieke individue te identifiseer; die insameling en gebruik van sensitiewe inligting, soos byvoorbeeld mediese en finansiële data; die hoeveelheid inligting wat ingesamel en gebruik word; sekondêre gebruik van inligting; die gebruik en verspreiding van onakkurate databasisse; en die insameling en gebruik van verbruikersinligting om finansieël voordeel daaruit te trek. Verbruikers het ook belang getoon teenoor elektroniese databasis bemarkingspraktyke as gevolg van die geheimhouding oor data insameling en gebruik. Die belang by privaatheid mag egter varieër afhangende van verbruikers se kulturele oriëntasie, ouderdom, persepsie van wat goeie bemarkingsetiek behels of die spesifieke metodes gebruik om data aangaande verbruikers te bekom. Daar kan onderskei word tussen verskeie verbruikersgroepe wanneer verbruikershoudings teenoor databasis bemarkingspraktyke en persoonlike privaatheid oorweeg word. In hierdie verband kan die tipiese Suid-Afrikaanse verbruiker geklassifiseer word as 'n pragmatis. Pragmatiste is besorg oor privaatheid tot die mate waartoe hulle blootgestel is aan databasisbemarkingsaktiwiteite. Die Suid-Afrikaanse databasis industrie is nog in die beginfase en soos die industrie groei en verbruikers meer ingelig raak, sal besorgdheid oor privaatheid heelwaarskynlik ook toeneem.

Dit is belangrik om die kwessies wat besorgdheid oor verbruikersprivaatheid veroorsaak aan te spreek en om oplossings te vind om volhoubare databasisbemarkingspraktyke in die

toekoms te verseker. Daar moet gepoog word om bemarkers se behoefte aan inligting en verbruikers se behoefte aan privaatheid in ewewig te bring om sodoende owerheidsinmenging te voorkom. Opofferings van beide partye is nodig om 'n meer gebalanseerde verhouding tussen die twee partye te bewerkstellig. Die suksesvolle uitkoms van die privaatheidsdebat sal afhang van bemarkers se begrip vir verbruikersprivaatheidskwessies en om dit dienooreenkomstig aan te spreek.

Die regulering van databasisbemarkingspraktyke wat inbreuk maak op verbruikersprivaatheid kan verskillend benader word: die implementering van inligtingstegnologie, self-regulering en owerheids-inmenging. Self-regulering word verkies as basis om databasisbemarkings-praktyke te reguleer, terwyl privaatheids-bevorderende inligtingstegnologie aanbeveel word as bykomende gereedskap om verbruikersprivaatheid te beskerm. Owerheidsregulering word gesien as die laaste uitweg as gevolg van onnodige beperkinge wat dit mag plaas op databasisbemarkingsaktiwiteite.

Die voorgestelde modelle vir die regulering van databasis bemarkingsaktiwiteite en vir die beskerming van verbruikersprivaatheid in Suid Afrika, is die Registrasie Model, tesame met elemente van die Data Kommissaris Model. Hierdie modelle is voorgestel nadat eienskappe, uniek aan die Suid Afrikaanse databasisbemarkingsindustrie, deeglik oorweeg is. Die modelle plaas die verantwoordelikheid van data beskerming in die hande van die databasisbemarker en die Suid-Afrikaanse owerheid, eerder as by die verbruiker. Die Registrasie Model en die Data Kommissaris Model blyk 'n uitvoerbare kombinasie vir implementering in Suid Afrika te wees, omdat hierdie modelle die feit inagneem dat Suid Afrikaanse pragmatiese verbruikers nie goed genoeg opgevoed en ingelig is oor die databasisbemarkingsaktiwiteite wat inbreuk maak op privaatheid nie. Hierdie kombinasie behels selde verbruikersdeelname en is daarom gepas by die tipiese apatiese aard van Suid Afrikaanse verbruikers.

Die Registrasie Model dien as 'n kennisgee-stelsel waar 'n agentskap, tans die Direkte Bemarkings Assosiasie van Suid Afrika, beginsels vir regverdige inligtingspraktyke ontwikkel waaraan geregistreerde databasisbemarkers moet voldoen. 'n Kommissie, 'n element van die Data Kommissaris Model, het mag om verbruikersklagtes te ondersoek, die ontwikkelling van databasisse aan bande te lê en om datapraktyke te hersien en advies te gee oor verbeteringe in die stelsels van data-insamelaars. Die kommissie kan ook ontwikkelinge

in inligtingstegnologie wat verbruikersprivaatheid bevorder, monitor. Die enigste probleem met hierdie modelle blyk te wees dat die agenstkap en die kommissie geen gesag het om te verseker dat beginsels en kodes van goeie gedrag afgedwing word nie.

Industrie self-regulering, tesame met 'n mate van owerheidsbeheer en die implementering van inligtingstegnologie blyk nuttig te wees om voldoende vlakke van verbruikers-privaatheid en data beskerming te verseker. Dié kombinasie kan moontlik 'n balans vind tussen Suid Afrikaanse verbruikers se behoefte aan privaatheid en Suid Afrikaanse bemarkers se behoefte aan verbruikersinligting.

ACKNOWLEDGEMENTS

I am sincerely grateful to the following persons for the role they played in the successful completion of this assignment:

- Prof N S Terblanche, my supervisor, for his support, constructive criticism and the enthusiasm he shows for the field of study.

- Mrs Elaine Ridge, for the care she took in editing the assignment.

- Mrs Cornelie Prins, for the professional formatting and general advice on improving the assignment.

- My family and friends, especially my mother Yolandé Visser and Albrecht Gantz, for their continued support, encouragement and interest in my studies.

- University of Stellenbosch for their financial assistance through bursaries, which made this study possible.

CONTENTS

CHAPTER 3

MARKETERS' VIEWS ON DATABASE MARKETING PRACTICES

CHAPTER 4

CONSUMER PRIVACY CONCERNS RELATED TO DATABASE MARKETING PRACTICES

CHAPTER 5

APPROACHES AND MODELS FOR REGULATING DATABASE MARKETING PRACTICES

CHAPTER 6

CONCLUSIONS AND A SUGGESTED MODEL FOR REGULATING DATABASE MARKETING PRACTICES IN SOUTH AFRICA

LIST OF TABLES

LIST OF ABBREVIATIONS

FTC	Federal Trade Commission	25
DMA	Direct Marketing Association	26
URL	Universal Resource Locator	28
ANI	Automatic Number Identification	29
EPIC	Electronic Privacy Information Centre	69
PICS	Platform for Internet Content Selection	70
OPS	Open Profiling Standard	72
P3P	Platform of Privacy Preferences	72
OECD	Organisation for Economic Development	77
CME	Center of Media Education	80
CARU	Council of Better Business Bureau's Children's Advertising Review Unit	80
NIIFT	The National Information Infrastructure Task Force	82
ICC	The International Chamber of Commerce	82
ECPA	Electronic Communications Privacy Act	88
CALEA	Communications Assistance for Law Enforcement Act	88
CDA	Communications Decency Act	91
PPM	Privacy Protection Model	95

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

"Privacy is like clean air – at one time there was plenty of it; now it's just about gone"

It is the opinion of Pincus and Johns (1997: 1237) that this anonymous quote can be applied to the concept of database marketing as it stands today. Database marketing practices invade consumer privacy like pollution does with clean air. Further growth and development of the database marketing industry would mean that consumer privacy would be threatened even more. Mechanisms need to be found to "clean the air from pollution" again. Applied within the database marketing context, this means that effective privacy protection measures need to be identified to ensure sustainable growth in the database marketing industry.

The concept of privacy can be traced back to early manhood, but the perspective that has been embraced by many courts and has guided much legislation, was originally proposed by Prosser in 1960 (Phelps, Nowak and Ferrell: 2000). Prosser suggests that privacy is a term that encompasses at least four different dimensions or legal torts, including intrusion, disclosure, false light and appropriation. The concept of privacy today still enjoys much attention and will most probably continue to in future.

The development of database marketing has been stimulated by advances in information technology, which started in the 1980's with the personal computer revolution (Federal Trade Commission, 1996). Database marketing practices mainly involve the collection and use of consumer information. Various reasons can be given for the increased popularity of database marketing. From the marketer's point of view, data from various sources are aggregated and then used to compile consumer data lists and databases. Data mining techniques are used to analyse such data and for identifying consumer wants and needs. The information enables marketers to segment consumer markets and to develop targeted advertising messages and customised products and services. Consumer information therefore improves the overall marketing strategy and results in more efficient marketing practice.

From the consumer's point of view, there are advantages, but more importantly many concerns for the use of personal information. Advantages of using consumer information include the availability of improved and more customised products and services and access to a wider variety of products and services. Consumers are concerned about privacy for various reasons. Consumers generally lack knowledge of data collection and use and are unaware of the type of information collected. The fact of having little control over subsequent use of data also raises privacy concern. Other factors that raise privacy concern include: the use of personal information to identify specific individuals; collection and use of sensitive information, such as medical and financial data; the volume of information collected and used; secondary information use; the use and dissemination of inaccurate databases; the collection and use of children's data and the perceived lack of benefits received in exchange for information provided. Consumers are also especially concerned about online database marketing practices because of the secrecy in data collection and use. Consumer privacy concerns however, may vary depending on consumers' cultural orientation, age, perception on what constitutes good marketing ethics, or exposure to database marketing practices.

Responses to consumer privacy concern include the application of privacy-enhancing information technology, industry self-regulation and government intervention through legislation. These approaches have varying degrees of success in protecting consumer privacy. Information technology could minimise the disclosure of personal information and empower the consumer to have more control on the collection and use of personal information. Industry self-regulation requires members of the database marketing industry to monitor data practices and to ensure that an adequate level of consumer privacy exist. Industry members have to comply with certain industry principles and codes of conduct to ensure that consumer privacy is maintained. Government intervention normally protects consumer privacy by means of legislative efforts. Legislation however, restricts marketers' innovation and creativity because it imposes strict laws on data practices. Government intervention seems to be the last resort for protecting consumer information.

Bennett suggested several models for the protection of privacy. These include the Voluntary Control Model, the Subject Control Model, the Licensing Model, the Registration Model and finally the Data Commissioner Model. These models indicate which parties - consumers through application of information technology, industry self-regulation or government - should be held responsible for monitoring and initiating privacy protection. Pincus and Johns proposed another model, namely the Privacy Protection Model. The value of this model lies

in its qualitative nature, which measures a country's level of privacy protection in relation to other countries by plotting a country on a continuum with endpoints, no privacy and complete privacy. Bennett's models and Pincus and Johns's model could be useful in evaluating an appropriate system for protecting consumer privacy and for evaluating the effectiveness of such a system.

1.2 OBJECTIVES OF THE STUDY

Database marketing enjoyed rapid growth over the past decade in countries such as the United States of America and in the European Union. The Direct Marketing Association of Southern Africa claims that the South African database marketing industry is still in its infancy phase. It is therefore believed that database marketing in South Africa, will in the very near future, also enjoy rapid grow. This study focuses on the problems related to database marketing, experienced by the United States of America. South Africa could learn from the experiences in more developed countries and could apply obtained knowledge to identify an appropriate model for protecting consumer privacy in South Africa.

General objectives of this study were to evaluate different database marketing practices that raise consumer privacy concerns from both a marketer and consumer point of view. The inherent advantages and disadvantages of using consumer information are being identified, also from both parties' point of view.

The primary objective of this study is to recommend an appropriate model of privacy protection for South Africa. Recommendations are based on the evaluation of available models, the successful implementation of these models in other countries and also characteristics unique to the South African environment. The appropriate model needs to protect consumer privacy, while ensuring continued growth in the South African database marketing industry.

1.3 METHOD OF INVESTIGATION

The method of investigation in this study was a literature overview. A comprehensive literature study of South African as well as foreign literature on all the possible aspects with regard to database marketing was undertaken. Sources of literature that were used in this study included books, articles, research papers, reports, publications on the Internet and other

relevant documents. Most of the literature used in this study was of foreign origin. The only material of South African origin that could be found on the subject of database marketing was publications by the Direct Marketing Association of Southern Africa. The literature study was done to obtain insight concerning the concept of privacy, database marketing practices, consumer privacy concerns and available approaches for protecting consumer privacy.

1.4 STRUCTURE OF THE STUDY

The study is presented as follows:

Chapter One serves as the introductory chapter and provides the background of the study, the main objectives of the study, the methodology and the structure of presentation of this study.

Chapter Two deals with a literature overview on different concepts of privacy. This chapter refers to three meanings attached to privacy. The general meaning of privacy is concerned with territoriality or an individual's need for physical seclusion. Legally, privacy is accepted as a human right worth protecting. Legal entities have adopted certain privacy torts and today acknowledge an individual's physical and information privacy. The last part of this chapter refers to consumer privacy. Consumer privacy mainly focuses on privacy of a consumer's information. The concept of consumer privacy is most relevant to the rest of this study.

Chapter Three briefly refers to the impact of information technology on the development of database marketing. This chapter is mainly concerned with database marketing activities from the marketer's point of view. Different data collection methods as well as the value of consumer information for database marketers are discussed.

Chapter Four addresses consumer privacy concerns that result from database marketing activities. This chapter starts by referring to different consumer clusters, measured on a scale for privacy concern. An overview on the typical South African consumer, with regard to database marketing activities, is given. A detailed discussion of consumer privacy concern with regard to database marketing practices, follow. Also, reference is made to factors that correlate with the level of consumer privacy concern. The final section of this chapter deals with possible trade-offs between efficient database marketing practice and consumer privacy concern. Recommendations are made on possible compromises by both parties to ensure a more balanced market environment.

In Chapter Five a discussion is given on the possible approaches for regulating database marketing practices and its effectiveness in ensuring an adequate level of consumer privacy. Privacy-enhancing information technology is described as the first approach to protect consumer privacy. An examination of industry self-regulation as second approach and government intervention as last approach to protect consumer privacy, follow. In the final section of this chapter, discussions focus on possible models, which combine different approaches, for protecting consumer privacy. Recommendations are made regarding an appropriate model for regulating database marketing practices in South Africa.

Concluding remarks with regard to all the issues discussed in earlier chapters, are given in Chapter Six. In this chapter, a more detailed evaluation is made of available models for protecting privacy. A recommendation is made on an appropriate privacy protection model for South Africa. This chapter also discuss the various reasons that support the recommended model(s). The last section of this study refers to some suggestions and possible objectives for future research.

CHAPTER 2

THE CONCEPT OF PRIVACY

2.1 INTRODUCTION

The concept of privacy dates back to early mankind. Over time there were various meanings attached to privacy but the basic principle, which is the need for privacy, stayed the same. The concept encompasses three meanings when examined from different viewpoints. Although these meanings may overlap, reference to the following three perspectives will be made:

- The general meaning of privacy;
- Privacy as defined by law; and
- Privacy within a marketing context.

2.2 THE GENERAL MEANING OF PRIVACY

The general meaning of privacy mainly refers to one's physical privacy or territoriality, and acknowledges that privacy within different cultures will have different meanings.

2.2.1 Territoriality

When considering privacy's general meaning, one likes to think that one's desire for privacy is distinctively human, and a function of one's basic needs. However, studies of animal behaviour and social organisation suggest that one's need for privacy may well be rooted in one's animal origins, and that humans and animals share several basic mechanisms for claiming privacy among their own kind (Westin, 1967: 8).

Westin (1967: 8) referred to animal studies, which indicated that virtually all animals seek periods of individual seclusion or small-group intimacy. This is usually described as the tendency toward territoriality, in which an organism lays private claim to an area of land, water, or air and defends it against intrusion by members of its own or other species. These territorial patterns serve a few important purposes within the animal environment. First, it will ensure procreation of species by regulating access to available resources. Second, these territorial patterns will enhance selection of "worthy males" and provide breeding stations for animals that require male assistance in raising the young. Third, it also provide a physical

frame of reference for group activity such as learning, playing, group interaction, and hiding against the entry of intruders. The parallels between territory rules in animal life and trespass concepts in human society are therefore that in each, the living being lays claim to private space to promote individual well being and small-group intimacy (Westin, 1967: 9).

Animals and man also share distance-setting mechanisms to define one's territorial spacing within groups. McCroskey, Young, and Richmond (2000) have defined personal distance as "the distance that an organism usually keeps between itself and other organisms". Among species such as birds and apes, there are rules of "intimate distance" regulating the space held between them. "Social distance" links members of the animal group to one another in order to distinguish them from other groups, while "flight distance" is the point of approach at which an animal will flee from an intruder of another species. Although humans have eliminated flight distance as this is part of one's regular social life, Hall's studies indicate that one sets basically the same kinds of personal, intimate, and social distance in one's interpersonal relationships (Westin, 1967: 9).

When classifying human life spaces within the privacy context, the term "proxemics" becomes relevant. Much of the accepted science in this field is attributed to anthropologist Edward Hall, who defined proxemics as "the interrelated observations and theories of man's use of space as a specialised elaboration of culture" (IP100 plug-in: Proxemics, 2000).

Hall (IP100 plug-in: Proxemics, 2000) categorised interpersonal spaces into the following categories:

- Intimate - from zero to 0,5 meter
- Personal - from 0,5 to about 1,3 meter
- Social - from 1,2 - 3 meters
- Public - from 3 meters up

There are also several other variables that influence man's perception of a private zone. A study undertaken by McCroskey et al (2000) identified the following variables that have an influence on the use of space to define one's private territory: sex, race, superior-subordinate relations, familiarity, degree of friendship, status, interaction setting, physical appearance, and desire for approval. However, while research to date has generally been supportive of the idea of space differences, the exact nature of such differences is not clear.

2.2.2 Cultural differences

The interpersonal zones, which were referred to in paragraph 2.2.1, will vary when considering different cultures and different contexts. The personal zones that people attach to certain things will thus vary according to one's culture and what zone distances different cultures perceive as acceptable. Generally it has been said that, low context cultures, such as Americans, have a tendency to have further distances than high context cultures, such as the Chinese (What are haptics and proxemics?, 2000). However, it is important to note that not everyone in the same culture has exactly the same perspective on what the appropriate distance within a giving situation will be. People tend to be different in many aspects and will thus vary according to individual needs (IP100 plug-in: Proxemics, 2000).

The differences in cultures' perception on appropriate interpersonal distances are the result of differences in historical and political traditions as well as social settings amongst them (Westin, 1967: 26). However, all societies seem to provide privacy of some kind to members, although what is considered to be private, and the mechanisms used to control privacy would vary across cultures (Petrison and Wang, 1995: 20).

In order to explain cultural differences, one could refer to the British and American perspectives on privacy as an example. Britain is typically a small country with a relatively homogeneous population, strong family structure, positive public attitude toward government, and elite systems of education and government service. This combination has produced a democracy in which there is great personal reserve between Englishmen, as well as high personal privacy in home and private associations (Westin, 1967: 26). Privacy for the British seems to have been treated as a philosophical issue, to be resolved with the development of general principles that apply to a wide variety of situations (Petrison and Wang, 1995: 34). Americans tend to take a relativistic approach to the issue of privacy where specific potential infringements are judged on an individual basis in terms of the harm it is likely to bring about. The given situation or circumstances may influence what American's perceive as an invasion of privacy. Therefore, America lacks a coherent system that stipulates criteria for invading one's privacy. Compared to the British, Americans seem relatively unconcerned about protecting informational privacy (Petrison and Wang, 1995: 33).

Thus, even for two countries that have as much in common as the United States of America and Britain, privacy seems to be associated with different sorts of values, and what is

construed to be a privacy invasion seems to differ significantly across the two cultures. These differences may be attributed to the immediate social influences present in each country at a particular point in time, such as the greater amount of marketing activity in the United States of America, or to more general preferences that vary by culture (Petrison and Wang, 1995: 34).

2.2.3 Valuing privacy

The concern for privacy in various aspects of life is fundamental to human existence. Valuing privacy in its various forms is a very basic component of one's live. Privacy is, to some extent in conflict with other human needs. A competitive environment exists when an individual has to decide whether to grant privacy priority over other human values and interests. In reality, the greater one's exposure in public, the less privacy one can continue to expect, claim and enjoy (Flaherty, 1998). Although individual animals and humans have a need for privacy, one would not be able to function without social stimulation. Therefore, the idea is not to achieve absolute privacy but rather to achieve a balance between privacy and the need for social interaction (Westin, 1967: 13).

2.3 THE LEGAL MEANING OF PRIVACY

Law enforcement for protecting consumer privacy is not widely implemented. There is some statutory legislation for data protection as well as for some areas of privacy, but few are directed at consumer privacy itself. Common law acknowledges privacy as a human right and several countries have developed a Bill of Rights where the general right to privacy is acknowledged. The relevant laws and legislation will be discussed in Chapter 5. At this point it is appropriate to examine the legal meaning for privacy.

2.3.1 The Bill of Rights

De Waal, Currie and Erasmus (1999) undertook extensive research on the interpretation of privacy as implied by the Bill of Rights. The South African Bill of Rights, as well as its international counterparts, provides for the recognition of privacy as a human right worth protecting. This particular right, is only concerned with the general right to privacy and do not refer to specific consumer privacy rights. Article 14 states the following:

"Everyone has the right to privacy, which shall include the right not to have -

- their person or home searched;
- their property searched;
- their possessions seized; or
- the privacy of their communications infringed".

Section 14 has two parts. The first protects a general right to privacy, while the second protects against specific infringements of privacy. Usually, the two parts are dealt with in separate sections of the Bill of Rights. In South Africa, however, the specific areas of protection form part of the general right to privacy (De Waal et al, 1999: 253-254).

Section 32(1) of the Bill of Rights guarantees the right of access to information held by the State, and to information held by another person that is required for the exercise or protection of any right. The Bill has been extended to include a chapter relating specifically to the rights of privacy and information access in the private sector. The objectives of the Bill are to provide for: "...access by individuals to information about themselves held by private persons, the correction of personal information held by the state or private persons, and the protection of individuals against abuse of their personal information by the state or other private persons" (Direct Marketing Association: The privacy file, 1998). This implies that database marketers should allow for consumer access to personal information. Consumers should be granted the opportunity to correct personal information about them and also have some input regarding the secondary use of such information. Provisions like these have been adopted in industry codes and principles. These will be discussed in Chapter 5 under the heading self-regulation.

2.3.2 The common law right to privacy

South African common law stems from the Roman-Dutch law. Both law systems acknowledge the right to privacy as an independent personality right, which the courts consider to be part of the concept of *dignitas*. A breach of the privacy right occurs when there is an unlawful intrusion on the personal privacy of an individual or an unlawful disclosure of private facts about an individual. When determining the unlawfulness of a factual infringement of privacy, it is judged in the light of the general sense of justice of the community as perceived by the court, in law terminology better known as *boni mores* (De Waal et al, 1999: 254).

Typical examples of unlawful intrusions and disclosures include entry into a private residence, listening in to private conversation, the disclosure of private facts, which have been acquired by a wrongful act of intrusion, and the disclosure of private facts in breach of a relationship of confidentiality. When determining whether an invasion of the common law right to privacy has taken place, one should essentially assess whether the invasion was unlawful. The presence of a ground of justification (such as a statute) means that an invasion of privacy is not a wrongful clause (De Waal et al, 1999: 255).

The common law in a number of countries, such as England for example, does not recognise a general right to privacy and England have been resistant to introduce a broad statutory right. The English argued that the right is too difficult to define satisfactorily and therefore is far too broad to incorporate in their law. However, the traditional tort claims, identified by William Prosser are recognised in England. These will be discussed in paragraph 2.3.4.2 (Birks, 1997: 1,3).

2.3.3 The scope of the constitutional right to privacy

The constitutional right to privacy acknowledges a person's legitimate expectation of privacy, while taking into consideration society's expectation of privacy. In addition, the constitutional right to privacy seeks to protect three related concerns. These concerns are attended to in a later section.

2.3.3.1 Legitimate expectation of privacy

One has a legitimate expectation of privacy only where the scope of one's privacy right extends to aspects of one's life. A legitimate expectation means that society recognises the expectation of privacy as objectively reasonable. The so-called "reasonable man" principle can be applied where society determines what constitutes a reasonable amount of privacy. The subjective expectation of privacy recognises that one cannot complain about an infringement of privacy when explicitly or implicitly consented to having one's privacy invaded. For example, when a consumer provides information voluntary it cannot be seen as an invasion of privacy when the database marketer target the consumer with products, services or promotions that were developed with such information at hand. It is, however, difficult to assess the kinds of privacy expectations society would consider as objectively reasonable. For example, an individual provides information required to complete a

transaction, but it is then also used for purposes not necessary for the transaction (De Waal et al, 1999: 255).

The Constitutional Court in South Africa (De Waal et al, 1999: 256) has provided some guidance in this regard. In Bernstein v Bester {1996 (2) SA 751 (CC); 1996 (4) BCLR 449(CC)}, Ackermann J held that the scope of the right to privacy has to be defined with respect to the rights of others and the interests of the community:

> "The truism that no right is to be considered absolute implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly".

The constitutional right to privacy seeks to protect three related concerns and these rights are discussed below.

- The right to be left alone

First, privacy protects certain aspects of one's life where one is entitled to be left alone, such as one's body, certain places like one's home and certain relationships, such as marital, sexual or other intimate relationships. The rationale behind this right is to keep the state and other people out of one's private affairs. In legal terms, this right to privacy recognises that everyone is entitled to an environment of personal autonomy in which the law may not interfere (De Waal et al, 1999: 257).

- The right to development of the individual personality

Second, the right to privacy aims to protect the opportunities for an individual to develop a personality and therefore extends to certain forms of individual and personal self-realisation or self-fulfilment (De Waal et al, 1999: 257). Therefore, at the personal level, the right to privacy protects one's right to be or become the kind of person one wants to be. The

implication is that the state or anyone else may not force an individual to conform to a stereotypical view of what an ideal citizen should be. The right to privacy dictates that the state and society should be tolerant towards non-conformists. This aspect of privacy covers a vast terrain of human behaviour, and includes, for example, the clothes one wears and the manner in which one speaks or relates to each other (De Waal et al, 1999: 263).

- Information privacy

Thirdly, the right to privacy seeks to protect the ability of individuals to control the use of private information about them (De Waal et al, 1999: 257). This right is related to the protection of human dignity. It guarantees a person the right to control the use of all private information whether or not the information is potentially damaging to a person's dignity. The right is closely related to the right to dignity since information which places a person in a false light, is most often damaging to the self-respect of that person (De Waal et al, 1999: 263).

In Mistry v Interim Medical and Dental Council of South Africa {1998 (4) SA 1127 (CC); 1998 (7) BCLR 880 (CC)}, the Constitutional Court (De Waal et al, 1999: 263-264) considered the following factors relevant to the informational right to privacy: Whether the information was obtained in an intrusive manner; whether it was about intimate aspects of one's life; whether it involved data provided by an individual for a specific purpose, but was used for another; whether it was disseminated to others from whom one could reasonably expect such private information to be withheld.

2.3.4 Development of a privacy construct

There are many definitions of privacy from a legal perspective. The definitions recognise different dimensions of the concept of privacy and reference to each will be made in the following section.

2.3.4.1 Perspectives on privacy

In their 1980 landmark article, "The Right to Privacy," Warren and Brandeis (Culnan, 1993: 343) first articulated the need to secure for the individual's "right to be left alone". This view, are too broad to provide much guidance, but is applicable within the database marketing context for two reasons. First, it recognises that privacy encompasses an individual's desire for physical solitude. Therefore, a loss of privacy occurs when others do not respect a

person's realm and affairs, a perspective often shared by recipients of uninvited and unwanted direct mail and telephone solicitations. Second, this definition lays the foundation for many of the common law principles that recognise privacy as an individual right worth granting and protecting. This acknowledges the non-physical injuries such as harm to reputation and it provided an early foundation for the assertion that one should own the "facts relating to one's private life" (Nowak and Phelps, 1995: 48).

Westin (Nowak and Phelps, 1995: 49) emphasised informational privacy in a definition of privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Stone and Stone (Nowak and Phelps, 1995: 49) defined privacy as "a state in which an individual has the ability to control the release or subsequent dissemination of information about him or herself; regulate the amount and nature of social interaction; and to exclude or isolate him or herself from unwanted auditory or visual stimuli". Similarly, Culnan (Nowak and Phelps, 1995: 49) defined privacy as "the ability of individuals to control the access others have to personal information about them". From this perspective, unwanted direct mail or telemarketing calls are symptoms that arise from the inability to control the secondary use of personal information by third parties.

Dickler further expands the concept of privacy, and states that privacy holds three rights (Nowak and Phelps, 1995: 49):

- a right to publicity - which prohibit the unauthorised appropriation of one's name or image;
- a right of seclusion - which shields people from unwanted intrusions such as exposure to offensive products or services; and
- a right to keep private facts private.

Van den Haag (1971: 149) defined privacy as the exclusive access of a person (or other legal entity) to a sphere of it's own. The right to privacy entitles one to exclude others from (a) watching, (b) utilising, and (c) invading one's private sphere. However, Van den Haag suggested that the protection of privacy and the enforcement of laws generally, require sacrifice of one right for another or for the rights of others. Therefore, the rights of individuals and the duties of law-enforcement must be balanced against each other.

2.3.4.2 Legal torts of Prosser

The uncertain constitutional standing, along with a century of court rulings, scholarly and legal discussions, together with legislative actions, has codified the notion that privacy is not a unified or singular concept. Instead, it is a term that encompasses at least four different dimensions or discrete legal torts, which was originally proposed by Prosser in 1960 (Phelps, Nowak and Ferrell, 2000). These legal torts and examples thereof include:

- intrusion (physically invading a person's seclusion or solitude)
- disclosure (publicly disclosing embarrassing private facts)
- false light (false public portrayals)
- appropriation (use of a person's image or identity without permission)

This four-dimensional perspective, which has been embraced by many courts and has guided much legislation, has at least two major implications for marketing. First, it severely limits, if not completely eliminates, the legal applicability of the privacy concept to information practices that use market-level, rather than individual-specific, data according to Nowak and Phelps (Phelps et al, 2000). Legally, only information practices that involve the use of individual-specific consumer information are recognised as being a privacy concern (Nowak and Phelps, 1995: 49). Second, Nowak and Phelps suggest that most marketing uses of personal data do not constitute a tort of invasion of privacy. Legal interpretations combined with the difficulty of showing actual harm, suggest that intrusion, public disclosure, and false light have little judicial relevance to database marketing practices. Only appropriation is considered to be a viable dimension of privacy (Phelps et al, 2000).

One should consider the legal relevance of Prosser's framework when applying it to database marketing. The legal relevance of these privacy torts are discussed in the following sections.

- The legal relevance of intrusion

Prosser's four-part analysis retains much of its relevance in evaluating database marketers' practices relating to the gathering and use of individual-level consumer information. Two factors considerably reduce the legal relevance of the intrusion dimension of privacy to database marketing. First, although some data-gathering practices take place inside consumers' homes or involve physical measures, the knowing and willing co-operation of consumers eliminates the primary basis for an intrusion claim. Second, the fact that individuals' data are frequently used at a group level further reduces intrusion's applicability.

The concept of intrusion has been primarily restricted to privacy issues involving one's physical being. Intrusion can only be a real issue when the invasion was truly private; there must be no valid reason for the intrusion; and the intrusion itself must be highly offensive to a reasonable person (Nowak and Phelps, 1995: 50). The scope of the right is clearly limited by the relative importance of the countervailing interest in the intrusive behaviour. According to Nowak and Phelps (Phelps et al, 2000) intrusion claimants have the responsibility of proving that marketing practices have intruded on their physical being. However, consumers' ability to alleviate the unwanted intrusion quickly (e.g., throw unwanted mail away or hang up the telephone) questions the viability of such claims.

- The legal relevance of disclosure

Prosser's second tort, public disclosure, can also be excluded from most database marketing practices. At a minimum, the disclosure of private facts without the consumer's consent must be "highly offensive and objectionable" to a person of ordinary sensibilities according to McCarthy (Phelps et al, 2000). The collection and dissemination of individual-level information related to sexual relations or personal illnesses would therefore increase the viability of such claims. The specific relationship between two parties may also lay the foundation of the legal basis for confidentiality claims that may exist (Nowak and Phelps, 1995: 50).

- The legal relevance of false light

The third tort, false light, will also be difficult to substantiate because one has to persuade the courts that privacy concerns outweigh free speech considerations. Therefore, the applicability of false light within a database marketing context does not hold much relevance (Nowak and Phelps, 1995: 50).

- The legal relevance of appropriation

Prosser's fourth tort, appropriation, is the dimension of the privacy concept that has the strongest, most widely accepted legal foundation. It also appears to be the privacy dimension most directly related to database marketers' collection and use of individual-level information. Appropriation can be expanded to encompass database marketing practices that involve the use and dissemination of individual-level information, for example, list renting (Nowak and Phelps, 1995: 51). In general, the argument is that if one has some control over the reproductions and use of one's data, one should also be able to exercise some control over the

specific personal facts which one provides during the continuous business transaction (Phelps et al, 2000).

To conclude, Prosser's framework suggests that from a legal standpoint, only two dimensions of the privacy concept are applicable: appropriation and to a lesser extend, disclosure. Appropriation because database marketers use and disseminate individual-level information. Marketers' practices would not be actionable in case of the collection and use of general and group-level consumer information. Disclosure because database marketers' information practices may be actionable only to the extent where highly personal information regarding specific, individually identified consumers are inappropriately used or disseminated (Nowak and Phelps, 1995: 51).

Privacy can be viewed as a multidimensional concept due to the continuous provision of personal information as part of the exchange for goods and services. Therefore, in today's world of marketing, definitions such as "the right to be left alone" or "the right to unilaterally control information about oneself", are no longer feasible characteristics of privacy. Rather, when addressing consumer privacy concerns, one must rely on different perspectives (Nowak and Phelps, 1995: 51-52).

2.4 CONSUMER PRIVACY

A third viewpoint on privacy exists within the marketing context. Database marketing practices, which involve the collection and use of consumer information, sometimes invade consumer privacy.

2.4.1 Definition of a consumer

For the purposes of this study it is appropriate to begin with a broad definition of a consumer. A consumer, in the broad sense, could be "any person who is affected by the use of goods or services, whether or not he or she bought, hired or used them". In the narrow sense a consumer can be regarded as "any person who buys or hires goods or services, or any person who uses such goods or services" (McQuoid-Mason, 1997: 1).

The English dictionary defines a consumer as "one who purchases goods or pays for services", or "one who uses a commodity or service". Legal and commercial dictionaries

refer to consumers as "individuals who purchase, use, maintain, and dispose of products and services", or "members of that brand or class of people who are affected by pricing policies, financing practices, quality of goods and services, credit reporting, debt collection, and other trade practices". In essence, these definitions indicated that the word "consumer" includes everyone who buy or hire goods or services, everyone who use such goods or services and everyone who are affected by the use thereof (McQuoid-Mason, 1997: 1-2).

Westin's definition of consumer privacy has been well accepted by many consumer-rights groups. He defined privacy as "the claim of individuals, groups and institutions to determine for themselves, when, how, and to what extent information about them is communicated to others" (The protection of privacy, 2000). Westin (Culnan, 1993:345) argued that the key consumer privacy issues are to define fair information practices that are generally accepted by consumers, and how these practices can be institutionalised.

2.4.2 Physical privacy

In the database marketing context, privacy has two distinctive components: physical privacy and information privacy. Bennett (Culnan, 1993: 344) as well as Stone and Stone (Culnan, 1993: 344) proposed that a state of privacy exist, when a consumer can control social interaction, unwanted external stimuli, and the dissemination of personal information as well as making independent decisions without outside interference. On the other hand, it has been suggested that invasions of privacy occur when consumers are unable to control interactions with the social and physical environment or when actions are unknowingly structured. Typical examples of where an "invasion" of physical privacy exist, is when consumers receive unwanted telephone calls, mail, or direct sellers in their home (Phelps et al, 2000). The invasion of physical privacy give rise to many consumer debates, which may possibly lead to unnecessary laws and regulations that will threaten to dampen market economies and consumer choice, which result from more efficient uses of consumer data (Cespedes and Smith, 1993: 10).

2.4.3 Information privacy

In contrast to physical privacy, information privacy focuses on the collection, use and dissemination of personal information by a data user (government or a private entity such as a

database marketer) without the consent of the data subject (individual to whom the information directly refers, such as a consumer) (Blosh, 1997).

Prosser (Phelps et al, 2000) suggested that both consumers and marketers often perceive privacy issues in terms of information control. This involves the control over who has access to one's personal data (i.e., disclosure), how personal data are used (i.e., appropriation and false light), and what volume of advertising and marketing offers arise from the use of personal data (i.e., intrusion). Consumers can only influence how information about them is used, when having a high degree of information control. Conversely, little or no information control means that consumers have an insignificant influence on the collection and use of personal data. When consumers have little information control, privacy may become infringed according to Larsen (Phelps et al, 2000).

Although information privacy is more complex than physical privacy, Cespedes and Smith (1993: 10) believe that it is ultimately the more important area for both marketers and public policy makers. The situation is considered to be complex because consumers and marketers disagree about who "owns" the data and what kinds of trade-offs acceptable should be in different situations.

Although the concept of consumer privacy has several definitions, it is quite clear that most of consumers' privacy concerns relate to the exchange of personal information. Culnan and Milne suggested that privacy could be seen as an implied social contract (Phelps et al, 2000: 5). The presumption is that a social contract exists when a consumer provides a marketer with personal information. When this social contract is breached, it can also be seen as an invasion of privacy. The contract is breached according to Culnan if consumers are unaware that information is being collected; if the consumer's personal information is disseminated or rented to a third party without permission; or when consumers are not given an opportunity to remove their names from databases. Therefore, two key assumptions to consumer privacy are that (1) most consumers would like to have more control, and (2) giving consumers more control over how information is used will alleviate consumers' privacy concerns (Phelps et al, 2000: 5).

2.5 THE VALUE OF PRIVACY

A large volume of literature exists on the value of privacy, its role in social life and the various meanings attached in different cultural settings. Although the concept of privacy may be difficult to define or to explain why one need it so badly – a person have intuitive feelings that one cannot function as a human being without at least some degree of privacy. Bathing, sleeping, courtship, and other personal activities are almost always to some extent hidden from public view.

Privacy serves a number of values such as one's need for space and time for self-observation. It enables an individual to get away from the public and social environment and to release feelings and emotions that cannot appropriately be expressed in public and social life (Birks, 1997: 6). Privacy is strongly related with concepts of freedom and liberty, and values such as dignity and autonomy. It has been said, that a free society is governed, in part, by the principle that: "There are frontiers...within which men should be inviolable, these frontiers being defined in terms of rules so long and widely accepted that their observance has entered into the very conception of what it is to be a normal human being" (Logsdon, 1980: 125).

When considering one's privacy there is always an underlying assumption that one's interests are balanced with those of society as a whole. Consumers are willing to give up a measure of privacy in exchange for some economic or social according to Laufer and Wolfe (Culnan, 1993: 344). It is evident that the need for privacy is a socially created need because without society there would not be a need for privacy (Moore, 1984: 73).

2.6 SUMMARY AND IMPLICATIONS FOR DATABASE MARKETING

This chapter referred to three meanings attached to the concept of privacy. First, reference was made to the general meaning of privacy that acknowledges that all humans desire some degree of territorial privacy. Secondly, the legal interpretation of privacy suggests that privacy is a human right worth protecting, although not always explicitly adopted in legislation. Legal definitions of privacy acknowledge privacy of the person (physical privacy) as well as privacy of a person's information and communication (information privacy). Thirdly, reference was made to the concept of consumer privacy. Consumer privacy focuses primarily on privacy of a consumer's personal information. The concept of consumer privacy

is most relevant for this dissertation but one should also consider the influence the other meanings of privacy might have on consumer privacy.

Different aspects of a person's privacy were addressed in this chapter. Literature suggests that all human beings, whether human or animal, have a need for personal privacy. This was referred to as territorial privacy. Everyone has personal space zones, which another being should respect. Consumers believe, however, that marketers through data practice, such as data collection by means of telephone, intrude on personal, social and public spaces. Legally, however, most of these data practices are accepted and widely employed. It is especially the voluntary nature of data provision by consumers that limit the legal applicability of privacy invasion claims.

The legal definition of privacy holds implications for the regulation of database marketing information collection and use activities. Currently, few laws and legislation are in place in South Africa to regulate such activities. Statutory law, common law and specifically the South African Bill of Rights recognise the general right to privacy. The Bill of Rights proposes that individuals should have access to information held about them; should be able to correct incorrect information; and should have some protection against the abuse of such information. This implies that database marketers cannot use consumer information as they please, but should keep the rights of consumers in mind when collecting or using personal information. Marketers could study the particular legislation, common law or certain accepted practices before entering a market. This will enable database marketers to determine whether practices comply with the area's norms. Database marketers need to develop codes of conduct that reflect legislative definitions of privacy. Marketers could then employ legitimate data practices to alleviate consumer privacy concerns. The lack of coherent and specific data protection or consumer privacy protection laws in South Africa may, however, result in little concern for consumer privacy by marketers.

Generally, the legislature acknowledges privacy as the right to be left alone; the right to the development of an individual personality; and the right to informational privacy. However, consumers cannot expect to be left alone because they participate in society's exchange of goods, services and information. The right to the development of an individual personality is at stake when database marketing practices involve the collection and use of children's data. Children's data may be disseminated to third parties with harmful intentions and might be exposed to inappropriate or explicit database marketing offers. These practices are harmful to

a child's development of an individual personality because this material might influence vulnerable children. An invasion of information privacy occurs when marketers obtain personal data in an intrusive way. In addition, the right is concerned with secondary information use and the dissemination of data. This holds implications for marketers. If database marketing practices do not comply with the right granted by constitution, database marketing might face legal consequences.

The privacy construct, as one knows it today, has been developed since the 1890's. As discussed earlier, various definitions of privacy have been formulated, but there is still no universally agreed-upon meaning. Authors stressed mainly two points: informational privacy and physical privacy. These core dimensions of the privacy construct were extended by Prosser's legal torts, which are widely accepted by courts and legal entities. However, only two of the torts, namely disclosure and appropriation appears to be relevant within the database marketing context. The direct legal implication of disclosure for marketing practices is that highly confidential information, such as medical, financial or sexual information should be treated as such. Database marketers should be sensitive to consumer concerns especially when confidential information is involved. The direct legal implication for appropriation is that only the collection and use of individual-level information will be seen as an invasion of privacy and should be limited, especially where consumers have not granted explicit or implied consent to such data collection and use practices. Database marketers could however use group-level information without invading consumer privacy.

A further perspective on privacy relates to privacy from a consumer's point of view. Consumer privacy predominantly focuses on informational privacy, but in addition it also recognises physical privacy. Social interaction and the social environment, in which consumers participate, create the need for privacy. Consumers' need for privacy is therefore, in conflict with the need for social interaction and the need to participate in commercial exchange relationships. Consumers should weigh the social and economic benefits received in exchange for providing personal information, and accordingly decide what level of privacy are desirable. Complete privacy is not the ultimate goal, but rather consumers desire a reasonable level of privacy as expected by society. The constitutional right of privacy acknowledges that a person could expect a reasonable amount of privacy when participating within society. The more one interacts with other members of society, the more one could expect to compromise a certain amount of privacy. This implies that when consumers participate in a business transaction or where an exchange relationship exist (between

database marketer and consumer), consumers could expect that a degree of privacy will be lost because the seller of a product or service will require some information to complete the transaction. There exist a trade-off between one's need to interact socially and one's need to maintain privacy.

The reasonable-man principle becomes inevitable in determining when consumer privacy is being invaded. This reasonable-man principle led to problems for marketers because what is reasonable for one is not necessarily reasonable for another. This is especially a problem for database marketers that work within different cultural contexts or that market products and services globally. The meaning attached to privacy will differ across cultures and therefore what a culture perceives as fair and reasonable information practices will vary. Marketing practices employed in a certain country might be seen as offensive or invasive in another. The problem is however, that it is very difficult to define "fair information practice". Database marketers should therefore identify, which data practices are acceptable within a given society. Cultural differences were evident in the British-American example. Americans are much more receptive to database marketing practices than the Britons. Cultural differences are prominent in both consumers and database marketers and will also impact on different database marketers' views on acceptable marketing practice. Members within the database marketing industry may therefore have different views and this could impact industry codes of conduct. These issues will be discussed in Chapter 4 and Chapter 5.

CHAPTER 3

MARKETERS' VIEWS ON DATABASE MARKETING PRACTICES

3.1 INTRODUCTION

Marketers agree that the collection and use of consumer data is an essential part of effective marketing programs. Consumers, on the other hand, perceive these data practices as an invasion of privacy. Somehow, one needs to create a balance between what consumers perceive as being wrong and what marketers perceive as being right. This is difficult because both parties think judicial grounds support their respective thoughts. The aim of Chapter 3 is to give a better understanding of database marketing practices and the importance thereof for marketers to participate in today's information society. This chapter will firstly refer to the influence of advancements in information technology on marketing activities. Secondly, marketers' views on database marketing information collection and use activities will be discussed. This chapter will solely look at database marketing activities from the marketer's point of view. The consumer's view on these activities and the related issues and problems will be discussed in Chapter 4.

3.2 INFLUENCE OF THE INFORMATION AGE ON MARKETING PRACTICES

New and more advanced applications for information resulted in changes in marketing activities. Information is an important source in facilitating a competitive advantage within any industry. Businesses, but more in particular marketers, realised that without relevant consumer information, one would not be able to sustain a competitive advantage over other key players in the industry. Marketers are utilising consumer information to create better consumer profiles and to improve the overall marketing strategy. The utilisation of consumer information in databases for marketing activities, are better known as database marketing.

The following paragraphs will highlight specific global changes that affect database marketing activities. Reference will be made to the development of the personal computer, Internet and advancements in information technology, all of which have major implications for the collection and use of consumer information.

3.2.1 The Information Age

The information age is characterised by newer technologies, especially information technologies, which are employed to benefit governments, organisations and the general public. Information is seen as the key to success if an individual or a group is able to interpret and apply it in a meaningful way.

The changing information landscape started in the 1980's, when the personal computer revolution enhanced the abilities of governments, industries, and marketers to capture a vast amount of personal information automatically according to the Federal Trade Commission's (FTC) Staff Report (FTC: 1996). Next came the development of the Internet that expanded the possibilities for information exchange. The Internet was initially developed and used by only a small group of people in the academic and research community, but after 1990 it opened up for public use when the first "user-friendly" tools were developed: first Gopher and then the World Wide Web. Ever since its inception, the Internet user base has doubled every 12-18 months and millions of people are using the Internet as a personal and institutional communications system today (Coyle, 1998).

The development of the Internet has transformed methods of gathering, processing and sharing of information: methods, which were already transformed by the computer itself. As the Internet expands and new information technology develops, so does the potential to acquire and exploit personal information (Valentine, 1999). This is especially made possible by the ability of electronic mediums to reduce the effects of geography and time in disseminating information. Businesses, individuals, governments, and other entities are all contributing to this global information infrastructure. Database marketing technology and the Internet play an important role in database marketing activities. It is a very useful means for obtaining consumer data and the transfer of data became much quicker and cheaper than with more traditional methods for data collection and use (Grover, Hall and Rosenberg, 1998: 5).

3.2.2 The impact of information technology on marketing

Why is information technology an important development for marketing? The use of information has become an integral part of marketing. Specifically it led to database marketing, which relies on detailed consumer information for all marketing programs. The more information, the more accurate are marketers able to target consumers. Information

technology also provides a stimulus for change, which have implications for new marketing techniques and the collection, processing, storage and use of information that are essential to database marketing. These are all reasons why the development of information technologies, as well as the Internet with its possibilities to acquire information in a unique way, is of such importance to marketing. Specific reference will be made in paragraph 3.3 to the benefits of information for database marketing activities (Saxby, 1990: 3).

Dempsey (1997) identified some of the following broad technological-related trends that affect database marketing activities and the protection of consumer privacy.

- The rapid expansion of wireless services, which are increasingly used in business applications and by ordinary citizens for personal conversations, has made electronic communication almost totally flexible and constantly available. Yet, while offering attractive advantages of flexibility, wireless communications are less secure than traditional landline communications. Technology convergence is made possible by new information technology that allows the integration of computing, communications and sensory technologies. All of these enable marketers to transform information into data for sorting, manipulation, translation, transportation and storage (Pallante, 1998: 5).

- The globalisation of communications technology, information infrastructure and networks is breaking down national borders. Governments' control over information and technology became harder to maintain as a result of the irrelevance of borders, and yet, enforceable privacy protections have not emerged from the global information infrastructure.

Newer information technologies contribute to more effective database marketing activities and have also led to an increase in these activities. Database marketing, however, raise consumer privacy concerns, but as stated above, government cannot control the use and spread of these technologies. This will have significant consequences for determining an appropriate model for the protection of consumer privacy.

Information technology makes it possible for database marketers to develop relational databases that allow easy access to ever expanding internal and external consumer information sources. The Direct Marketing Association (DMA) of South Africa defined a database as "a computer-based repository of information organised in such a way as to allow

for efficient retrieval, manipulation and analysis" (DMA: Glossary of direct marketing terminology, 2000). Marketers are able to compile data from different geographical locations into a single meaningful consumer database. The captured data can be analysed to increase marketing efficiencies (Nowak and Phelps, 1992: 29).

Related to database marketing is responsive marketing where marketers have the ability to know customers, anticipate customers' needs and to respond accordingly. Responsive marketing has three elements: ongoing collection of data, interpretation of such data and application of the results obtained from data analysis. The database marketer is now able to extend the knowledge of each customer more than ever before and could keep the customer profile up-to-date (Harvey, 2000).

3.3 AVAILABLE METHODS FOR OBTAINING CONSUMER INFORMATION

Consumer data and information can be obtained from various sources. There are however, three major sources for obtaining consumer data. First, it is possible to obtain data through the marketing exchange process. Database marketers use a variety of methods to gather information from the marketing exchange process. Depending on the visibility and obtrusiveness of these methods, consumer concern will vary greatly. Nowak and Phelps (1995: 53) proposed the following general categories of database marketers' data collection methods: time/place of purchase; telephone inquiry; in response to advertising or promotion offers; surveys, studies, and questionnaires. More specifically, data collection take place when, for example, a mail or telephone order form is filled in, through loyalty clubs and product warranty cards, replies to direct response advertisements, as well as sweepstakes promotions and rebate redemption offers.

Secondly, consumer data can be obtained from public, proprietary, and government databases such as driver licenses and birth certificates. Consumers are relatively unaware of the importance of information obtained from these databases (Nowak and Phelps, 1995: 47).

Third, Grover et al (1998: 6) added electronic means, such as specialised tracking software as another major source for collecting consumer information. It is necessary to differentiate between online marketing exchange processes that involve gathering and use of consumer data and also third parties that collect and distribute such information for financial or personal gain.

These different sources of consumer data can be merged to obtain a better understanding and knowledge of consumer wants and needs. Detailed consumer databases enable marketers to develop consumer profiles that consist of specific information regarding consumer characteristics, lifestyle, buying behaviour and political and social activities (Nowak and Phelps, 1995: 47).

3.3.1 Information obtained through the marketing exchange process

The marketing exchange process involves several different methods by which consumer data can be obtained. These will be discussed in the following part of this chapter.

3.3.1.1 Financial transactions

Credit and debit cards that are used for daily purchases leave a vast trail of transaction records. Unlike with a cash transaction, it is possible for marketers to get hold of all transactions done by these cards. Detailed information on where products or services were bought, what day purchases were made and what specific products were actually bought, are available and obtainable. It is especially online credit card transactions that enable data collection (Froomkin, 1996). Consumers who purchase products online should determine whether the seller uses a secure connection. Such a connection begins with the universal resource locator (URL) "https://", instead of with "http://". Therefore, if the URL does not contain the "s", it most likely means the site does not have web security. In such circumstances anyone, including database marketers and even worse, third parties, may have access to a consumer's credit card and related details (Consumer privacy concerns on the Internet, 2000). The monitoring of daily and routine transactions, together with the possibility to collect vast amounts of consumer information has led to great consumer privacy concern (The end of privacy: The surveillance society, 1999: 19).

3.3.1.2 Smart cards

A smart card looks similar to a plastic credit card. The main difference however, is that it contains a tiny microchip that store consumer information. This device is used to pay for products or services and when swiped at the checkout counter, it records the consumers' purchased goods and other personal detail. Smart cards are especially being used for targeted database mailings and for relationship building (Bloom, Milne and Adler, 1994: 108).

3.3.1.3 Data collection by means of the telephone

Telemarketers typically collect detailed consumer information by requesting the data when selling products and services via telephone. It is quite obvious that telemarketers know the telephone numbers and names of individuals who are contacted, but additional information, such as credit card numbers or street addresses may be obtained. Privacy in this context is not really an issue because consumers provide information willingly to marketers. However, when considering telephone practices, such as 0800 numbers, automatic telephone number identification and electronic record-keeping systems, privacy becomes a more meaningful concern. In these situations, consumers lack knowledge of information collection and use (Nowak and Phelps, 1995: 54).

The following subparagraphs will refer to more specific telephone related methods applied to obtain consumer data.

- Automatic number identification systems

Automatic number identification (ANI) systems allow the party who is receiving a telephone call, to have the telephone number of the party who is calling displayed on a screen before the call is answered. Marketers use such systems to improve response times to consumer inquiries. Knowing the telephone numbers of consumers who have called can be of value when database marketers evaluate the impact of past promotional efforts or to develop more effective promotions in future. The list of names and phone numbers of people who have called, for example about product X, could also be used by marketers to identify buying patterns or such lists can be rented or sold to other third parties (Bloom et al, 1994: 108).

It is especially 0800 and 0900 numbers that are used to automatically identify incoming callers' telephone numbers. The data collected by these systems can be linked to other databases that contain personal information. This in turn, enables marketers to develop extensive consumer lists and databases (Nowak and Phelps, 1995: 54).

- Automatic diallers

Automatic diallers are computers that randomly dial telephone numbers. Once a number is reached, a pre-recorded message can be played, a fax can be sent, or a telemarketer can respond. Rather than dialling randomly, newer systems screen for disconnected lines, busy signals, and no answers, and will only connect the telemarketer when someone answers the

call. This minimises the time marketers have to wait between calls. Telemarketers sometimes obtain additional consumer information when completing a transaction via telephone. This information can be transferred to databases for further database marketing activities (Bloom et al, 1994: 108).

3.3.1.4 Data collection by means of the television

Data collection by means of the television includes methods such as interactive television screens and people meters. Videotext is a specific marketing tool used to obtain information by means of a computer. These methods of data collection will be addressed in the following subparagraphs.

- Interactive television

Interactive television viewing, which has already been implemented overseas, enable viewers to request, when convenient, detailed interactive information about a product or service. This interactivity will be made available during regular television commercials. Consumers can replace regular television commercials with interactive screens, by clicking a special button on the television remote control. Viewers can then request specific details about products or services or could fill out application and order forms right from the living room. The information on the application and order is collected and stored in the relevant marketers' database (Mainardi, 1997: 89).

- People meters

People meters are systems that monitor individual viewers to determine, which specific television programs they prefer watching. It is then possible to verify its audience through a camera device and matches the image with pre-recorded images of family members. The individual's identity, time watched, and television shows watched could be recorded. This information is mainly used to measure television audiences and for altering advertising related issues (Bloom et al, 1994: 107-108).

- Videotext

Videotext technology enables consumers to access a wide range of information regarding products or services by means of a personal computer. Hereby, companies gain access to individuals who are already interested in the company's specific product or service offerings.

Videotext relies on consumer interactivity and the information exchanged is recorded in marketers' databases (Bloom et al, 1994: 108).

3.3.1.5 Secondary sources of consumer information

Secondary sources of information collection typically involve information collected for one purpose and then used for other purposes. Database marketers or third parties, other than the original developers of consumer databases, gain access to the information sources mainly as a result of being involved in the marketing exchange process. The collection of such information may be consciously or incidentally. The most common collectors of this type of information are order fulfilment companies, shipping firms, financial transaction processors and credit card issuers. Secondary data sources result from database marketers' sharing of information, or having access to such databases (Nowak and Phelps, 1995: 52-53).

3.3.1.6 CD-ROM

CD-ROM's are used in a variety of settings, but relevant to marketing, one can consider it as a generation tool in a one-on-one discussion among prospects or consumers and a marketer. CD-ROM's are interactivity marketing tools, which can present information upon a viewer's request. This interactivity allows the user to enter personal information and receive customised and relevant product or service related information in return. This information can then be compiled in order to develop extensive databases (Mainardi, 1997: 88).

3.3.1.7 Other offline data collection practices

Marketers employ a variety of methods to collect information from consumers, offline. These include contests, sweepstakes, subscription forms, magazine surveys and promotional offerings, such as coupons or cash discounts. Some database marketing efforts aim at obtaining consumer information while offering a possible benefit. Although many consumers may be aware of the collection of such information, they might not know to what extend information is being collected or how such information is being used (FTC, 1996).

3.3.2 Public records

Many database marketers rely on personal and household information gathered by government departments and local municipalities. Public records include for example census data, vehicle registration records, driver and marriage license files, birth and death certificates, and property ownership records (Nowak and Phelps, 1995: 53). Privacy Inc's Consumer Privacy Guide (1998) suggested that military records and medical data from public hospitals should be added to public sources of personal information. Consider for example, drivers' licenses - it typically shows the owner's name, address, height, weight, age, and date of birth. Medical information, such as a driver's need for glasses may also appear on the driver's license. These records are often sold or rented for marketing purposes and have been described as "gold mines of personal information" (Froomkin, 1996).

3.3.3 Consumer information obtained through electronic means

As mentioned previously, electronic means for collecting consumer information are an important part of database marketing activities because it enables faster and cheaper collection of such information. Available online methods for obtaining consumer data will be discussed in subparagraphs 3.3.3.1 – 3.3.3.6.

3.3.3.1 Clickstream data

The Internet is a highly decentralised, global medium of electronic networks. It enables the collection and use of consumers' personal information. When users browse the World Wide Web, they leave an electronic marker, or clickstream, at each site visited. The clickstream data from each user's browsing activities can then be aggregated, stored, and re-used (FTC, 1996).

This information-gathering capability is built into the software that makes the Internet operate properly. The software automatically requires clickstream data to be collected or else it would be impossible for the data-receiving computer, to send out the information file requested by a user, to the user's computer, rather than someone else's. Therefore, clickstream data is an essential part in the functioning of the Internet (FTC, 1996). Clickstream data cannot really be linked back to personally identifying data but users still feel at unease because every move could be traced (Coyle, 1998).

3.3.3.2 Software

Loading software enables the running of an executable program (one ending in .exe) that can virtually read anything from the hard drive. Several hidden files can be loaded that could even allow others to run your computer and install new programs. This silent monitoring or lack of knowledge about information collection is a sensitive consumer issue. However, an Internet user could install "firewall" software to detect if the user is being traced and this program will alert the user when the computer communicates over the Internet (Being traced over the Internet, 2000).

3.3.3.3 Cookies

Although web users can be monitored in several ways, one method employed most often is a device called "cookies". A cookie is a file that is installed on a computer's hard drive under the individual's directory. This enables the person who installed the cookie (such as the online marketer or consumer profilers), to track what sites the individual (which uses that particular computer) visit and what the user does there. Therefore, the sites one visits as well as the products one buys are recorded (Grover et al, 1998: 6). Cookies combine all the information gathered on various web sites into a single record, and identifies when a user returns to a web site (Cranor, 2000). This enables the cookie to determine one's personal interests and draw conclusions about one's age, gender and buying habits (Consumer privacy concerns on the Internet, 2000). Cookies are often used to target or personalise advertising. For example, a site can use its cookie information to ensure that visitors do not see the same advertisements over and over again and advertisements can be correlated with the specific individual's preferences and interests (Coyle, 1998).

Third party cookies vary from regular cookies in that a third party marketer attempts to place a cookie on a consumer's computer by using another's web site. The third party database marketer normally places cookies on several different web sites to obtain a vast amount of information regarding homogeneous or heterogeneous consumer types. The majority of third-party cookies, which is placed on web sited, are from network advertising companies that aim to compile detailed profiles of consumers (FTC, 2000).

3.3.3.4 E-mail

Normally users can only be traced back to an Internet Service Provider, because after it reaches this destination, the e-mail is routed internally. However, web-based e-mail accounts display the real address of the Internet Service Provider and database marketers may then target or monitor the individual. This is made possible by for example, when a consumer opens an e-mail that contains a web page. E-mail addresses are often readily available in the form of existing consumer databases and it therefore provides easy access for database marketers. Marketers may use these e-mail addresses to send unsolicited mass mailings or to obtain additional information from users (Being traced over the Internet, 2000).

3.3.3.5 Web bugs

Web bugs are embedded in web pages or e-mail addresses that cause cookies to be transferred to others (Cranor, 2000). The Internet advertising community uses the term "clear GIF", rather than the term "Web bugs". The information that is sent to a server when a web bug is viewed, encompasses the IP address of the computer; the URL of the page that the Web bug is located on; the time the Web bug was viewed; the type of browser used; and a previously set cookie value. This information is typically added to a personal profile, which is identified by the browser cookie (Smith, 2000).

3.3.3.6 Online targeting of children

The Internet makes it easy, in comparison with traditional offline media, to collect information without the consent or knowledge of consumers. Database marketers, especially target young children for information collection purposes. Children are very willing to provide information when being promised to receive something tangible or intangible in return. Information collection techniques for children include correspondence with fictitious characters, signing a site's "guest book", registering with the site for continued access, and offering of incentives for completing surveys. Personal information may also be obtained from information requested as prerequisite for taking part in contests, bulletin boards, chat rooms, pen-pal services and online transactions. The collection of data from children increases daily because children are perceived as an easy target for these practices (FTC, 1996).

3.4 USE OF CONSUMER INFORMATION

Technological advancements have made it more economical to build databases, and easier to cross-classify information from different sources. About every marketer has access to such databases because it is becoming a necessity for effective marketing (Cespedes and Smith, 1993: 9).

Marketers that utilise databases are able to identify consumer groups, which previously have been missed or ignored. Marketers claim that traditional communication vehicles have become inefficient over time, while database marketing technology, offers more capabilities and promise. The problem is however, that with increased efficiency in marketing practices comes added responsibility towards consumer privacy concerns (Cespedes and Smith, 1993: 9).

The Privacy Inc' Consumer Privacy Guide (1998) stated that when considering information use in general, there are three primary uses for obtained information:

- Database marketing (for example, the compiling of mailing lists, and telemarketing),
- Background-checks (for employment and promotion, credit, loans, new-tenant screening), and
- Employee/workplace monitoring (for example, telephone and Internet use, and audio/video surveillance).

Each one of these areas of information use can be subdivided into more specific applications. However, only database marketing activities, and to a smaller extend background-checks, are relevant for this study. The following paragraphs will refer to several uses of consumer information for marketers that might raise consumer privacy concerns.

3.4.1 List compilation

Speedy and cheap access to large quantities of personal data, gathered in various places and at various moments, enables the compilation of consumer data lists (O'Leary, 1995). Marketers from American businesses view themselves as the sole owner of any information they have captured about a consumer. These lists are used for a variety of purposes, which range from segmenting consumers to renting or selling of consumer lists. These uses of personal

information will be discussed in separate paragraphs (Privacy Inc' Consumer Privacy Guide, 1998).

3.4.2 Data augmentation

Data augmentation is the process where companies purchase detailed information about consumers and prospects from secondary data sources. Computers match data obtained from these different databases to compile a single database with information about a particular individual or groups of individuals. In this format, the data provide a more complete consumer profile with information ranging from demographics, psychographics to life-style information (Bloom et al, 1994: 107).

3.4.3 Data mining

Consumer databases and lists are relatively worthless without proper analysing of such consumer data. Database marketers use "data mining" tools and techniques to identify trends and patterns regarding specific consumers or consumer groups (Privacy Inc' Consumer Privacy Guide, 1998). Data mining is the same as data analysis, where techniques like clustering and modelling are used to transform data into meaningful information. Data mining is used to predict consumer behaviour and to segment consumer groups (Loro, 1998: 24). Typical questions marketers attempt to answer when analysing databases, include: how much do consumers buy from the company and from which competitors; how likely are consumers to buy or re-buy from the company; how many units of a product is consumers likely to buy; what contribution a consumer may have to profits; and how much after-sale support the consumers will demand. The answers to these questions could only be answered after extensive analysis of databases that were compiled using various data sources (Weber, 2000).

3.4.4 Knowledge discovery

Marketers mainly use databases for knowledge discovery. Knowledge discovery from databases is the process of analysing large amounts of raw data to discover previously unknown and interesting facts about the data subject. Knowledge discovery significantly improves the marketing process because it enables marketers to generate more effective marketing campaigns and to improve individual customer service (Selfridge, 1995).

Marketers usually combine micro data, for example data on individual entities like consumers, companies, and transactions, to identify broad market segments and likely buying or consumption patterns and specific product or service preferences. Knowledge discovery does not aim at identifying specific individuals or entities because this would be a very costly and time-consuming process. The discovered group behaviour is attached to all members of the group when subsequently processing the discovered patterns (Kloesgen, 1995).

3.4.5 Segmentation of markets

After compiling consumer lists or databases, marketers are able to segment and profile consumer markets. It is important for marketers to determine the exact market segment for the relevant product; for example, a small niche market with specific needs or a broad market with general needs. Consumer profiles enable marketers to classify consumers into different market segments and assist in developing customised products and services (Nowak and Phelps, 1995: 54). Acquired data can thus be used to concentrate efforts on the most profitable consumers and to locate prospects that match the established consumer profiles (Morris and Pharr, 1992: 31).

3.4.6 Targeting

Marketers claim that personal information of consumers has greatly improved market segmentation, media selection and message creation. Therefore, the overall targeting of consumer groups have become much more efficient (Nowak and Phelps, 1992: 29). Once the target market is defined and the typical consumer profiles have been identified, marketers are able to create more efficient and targeted advertising messages that will reach the appropriate target market (Nowak and Phelps, 1995: 54). Database technology improves the efficiency and effectiveness of promotional approaches because marketers can sort through the available information and select the most appropriate marketing strategies and tactics (Bloom et al, 1994: 108). Marketers therefore waste less effort, money, and other resources by not promoting to individuals who are unlikely to react upon such an offer (Cespedes and Smith, 1993: 7).

3.4.7 Tailoring

Widespread databases assist marketers in offering products that are more reasonably priced and more precisely tailored for smaller, more homogeneous market segments (Morris and

Pharr, 1992: 30). Consumer databases are used to analyse consumer behaviour in order to develop more customised products and services. In addition, opportunities for new products or services could be identified (Hagel III and Rayport, 1997: 53). The more knowledge marketers obtain on the regular users of products or services, the better provision could be made in offering different variations of the product mix to more customer sets (Cespedes and Smith, 1993: 7).

3.4.8 Consumer satisfaction

As stated in the above paragraph, the use of consumer databases could lead to a wider variety of merchandise offers. This is due to the fact that detailed information regarding consumer groups may enable marketers to identify new gaps in the market. It is most likely that improved products and service offerings and access to a wider variety of products and services will result in higher consumer satisfaction (Phelps et al, 2000).

3.4.9 Loyalty

As stated earlier, the use of consumer data enables marketers to identify the best prospects for new products and services. Consumer information also enables database marketers to create promotions and reward programs that build consumer loyalty, by customising advertising and promotion strategies for the prospective customers (Phelps et al, 2000). By taking advantage of relationships the company has created through improved targeting and tailoring, it can develop and maintain better ties with consumers. Although consumers perceive direct mail as "junk mail", marketers view this as the initial building blocks of a long-term buyer-seller relationship. They argue that over time, consumers could expect to receive more relevant messages and products, and the company would be able to increase retention rates (Cespedes and Smith, 1993: 7).

3.4.10 Cost efficiency and increased productivity

Data collection and use practices are becoming more effective with the availability of information and database technology. It is cheaper and quicker to collect, aggregate and disseminate data by electronic means rather than with more traditional information collection methods. Database marketing utilise detailed consumer information in marketing programs

and as such are likely to result in increased productivity of marketing programs (Valentine, 1999).

3.4.11 Financial gain

Many companies collect consumer information for the purpose of selling or renting it to others for financial gain. This is a growing business today because these data lists and databases contain important information that most often reduce marketers' research costs and increase marketing efficiencies when applied effectively (Nowak and Phelps, 1995: 54). However, companies sometimes disseminate inaccurate, incomplete or irrelevant data although the buyer or renter of these may perceive it as being correct and handle it as such. This seems to be a problem, especially if consumers do not have the option to opt-out of secondary use of personal information (O'Leary, 1995).

3.4.12 Collection and use of sensitive information

The use of sensitive information enables marketers to create better and more accurate consumer profiles. Typical sensitive consumer information includes financial, medical, personal identifier and sexual information. As an example, reference will be made to medical information. As the health care industry changes, there is a move towards computerisation of patient records and electronic exchanges of medical information (FTC, 1996). The medical community has found these databases to be a tremendous asset according to Grover et al (1998: 8). It permits quick and easy access to needed information and consequently, improves the quality of health care services for patients (FTC, 1996).

Legally, these medical records belong to the doctor or the hospital that treats the patient. These records are distributed to a variety of institutions for purposes such as research and development of new or better products and services. Although patients lose some privacy, they gain by informed medical care when it may be needed most. Therefore, the medical community and database marketers justify the access to medical records (Grover et al, 1998: 8).

3.4.13 Collection and use of children's data

Children are very important to marketers because they represent a large and powerful segment of the marketplace. Children spend millions of dollars in the United States of America each year and have a great influence on the expenditure of others such as friends and parents (FTC, 1996). Therefore, advertising on kid-based Web sites has become a rapidly growing market for consumer companies, but it has also resulted in concerns for parents. Marketers use children's data for market research and specifically targeting purposes, but many critics question the appropriateness thereof because children lack the analytical abilities and judgement of adults when making choices. Children will therefore be unable to differentiate between information that should be kept private and information that could be provided to marketers. Database marketers often target children to obtain personal information regarding the parents of children (Austin and Reed, 1999: 590). Database marketers use Web sites to facilitate information exchange and communication back to a child and thus are able to develop a personal relationship with a child. This enables marketers to influence the buying behaviour of children, which may lead to increased sales (Austin and Reed, 1999: 591).

3.4.14 Inappropriate use of consumer information

Chapter 2 referred to several definitions of consumer privacy. In paragraph 2.4.2, Culnan (1993: 344) stated that consumers do not want to be exposed to unwanted visual and/or auditory stimuli. Marketers, or third parties that gain access to consumer databases, may use consumer information in a harmful way. For example, these parties could target consumers with inappropriate or explicit marketing offers either intentionally or unintentionally when consumers were wrongly categorised within a certain market segment. Marketers claim consumer databases are used to target relevant individuals or consumer groups. The Supreme Court of the United States recognises that this material may be accessed both intentionally and unintentionally, but claims that Internet users seldom encounter such adult content by accident. The assumption has been made that almost all sexually explicit images are preceded by warnings about the content and therefore, the 'odds are slim' that a user would enter a sexually explicit site by 'accident'. Furthermore, a child requires some sophistication and some ability to read and retrieve material and thereby would not be able to use the Internet unattended (Craig, 1998: 3-4). Such a statement is, however, highly debatable. Consumer perspectives regarding this issue will be discussed in Chapter 4.

Unsolicited commercial e-mail is another inappropriate use of consumer information. E-mail as communication medium was commonly used between businesses in the past, but it has also entered the private use area. Increasing amounts of e-mails are being sent from businesses to consumers and from consumers to businesses. Access to consumers' e-mail addresses, enables marketers to send mass mailings to promote products and service. E-mail is an informal, unstructured but highly efficient and cost-effective way to communicate with both consumers and prospective consumers. Unsolicited e-mails may contain useful information relevant to consumers' interests, but several unwanted spam messages are being forwarded to consumers. The spam messages consist of for example, common business opportunity scams, which promise vast income for a small investment of money and time; chain letters; and strategies for making money by sending bulk e-mailings. It is therefore, due to the special nature of the online marketing medium, possible to exploit ignorant consumers (Valentine, 1999).

3.4.15 Secondary use of consumer information

Secondary information use includes marketers who sell or rent consumer databases to third parties, mostly for financial gain. Marketers waste a lot of money when sending thousands of letters to individuals who have no interest in the offered product, service or cause. This problem was resolved by the compilation of detailed consumer databases. Consumer databases enable database marketers to identify a specific market segment for certain products and services and to identify prospective consumers who are most likely to buy the product or service offer. Marketers, rent or exchange lists of consumers, whose interests have been narrowed by previous purchase behaviour and other characteristics that could make them likely prospects (DMA: Frequent asked questions, 2000).

3.4.16 Background checks

Another use for consumer data, which has increased in popularity, is "background checks". This has become a faster and cheaper means for determining consumer creditworthiness. For example, a bank may review credit reports when a consumer applies for a loan or a retailer may consider credit reports before opening new accounts or grant credit (Privacy Inc' Consumer Privacy Guide, 1998).

3.4.17 Ownership of information

The question "who owns information?" has been asked numerous times. Marketers believe that they have developed consumer lists through database marketing activities and therefore the lists belong to them and they can do with it whatever they like. As a result, marketers argue that there is no need to get consumers' consent when selling or renting such lists (Taylor, Vassar and Vaught, 1995: 44). Take for example medical records hold by doctors. The consumer paid for the doctor's appointment (where the data is being collected) but, the doctor, may have paid for storage and interpretation thereof and therefore claim ownership of collected data (Selfridge, 1995).

Table 3.1 is a summarised example of marketers' data uses that raise several privacy concerns, but it refers specifically to Prosser's legal torts that were discussed in Chapter 2. Table 3.1 suggests that consumers are more concerned with database marketers' use of individual-level data than with group-level data. In addition, selling and renting of consumer information is a much higher privacy concern rather than the use of information for marketing purposes.

Table 3.1: Direct Marketers' Information Use Practices and Consumer Privacy

Level of information specificity	Data uses/Applications		
	Market and audience segmentation or profiling	Media planning and message design	Selling/renting consumer information to others
Individual-level, including:	**Potential Privacy Threats**		
Financial and credit data	Appropriation: • Little, or no input over whether, and how, information is used	Appropriation: • Little, or no input over whether, and how, information is used	Appropriation: • Little, or no input over information dissemination. • Little, or no, control over how information is used.
Lifestyle, hobbies, interests, and activities	False light: • Misclassification	Intrusion: • Misdirected or inappropriate advertising. • Loss of "right to be left alone".	Disclosure: • Public disclosure of erroneous or potentially embarrassing privacy facts. Intrusion: • Misdirected or inappropriate advertising. • Loss of "right to be left alone.
Group-level, including:	**Potential Privacy Threats**		
Inferred lifestyle, hobbies, interests, and activities Inferred values and attitudes Geodemographics Categorisations Broad demographic categorisations Broad geographic categorisations	False light: • Misclassification	Intrusion: • Misdirected or inappropriate advertising. • Loss of "right to be left alone".	Appropriation: • Little, or no input over information dissemination. • Little, or no control over how information is used. Disclosure: • Public disclosure of erroneous or potentially embarrassing privacy facts. Intrusion: • Misdirected or inappropriate advertising. • Loss of "right to be left alone"

Source: Nowak, G.J. & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: determining how and when "privacy" matters. Journal of Direct Marketing, 9(3), 55.

3.5 SUMMARY AND IMPLICATIONS FOR DATABASE MARKETING

The first part of this chapter focused on the influence of the information age on marketing activities. Information technology, especially computer information technology made society much more transparent. Advancements in information technology and the development and expansion of the Internet hold implications for marketing activities. It resulted in a shift from traditional marketing practices to concentrate on database marketing practices that involve the collection, processing and dissemination of vast amounts of consumer information. Marketers argue that the utilisation of detailed consumer information, are of utmost importance for effective marketing programs. Consumer information can now be obtained easier, cheaper and faster due to the availability of information technology. Consumer information is being manipulated, stored and applied to enhance marketing efficiencies. Most experts agree that personal information will increasingly become available to those marketers who wish to use it. Consumers also benefit from new information technologies. Database marketers are able to offer improved products and services, which are more customised than before. To the contrary, consumers also believe that personal privacy is being threatened by this readily available consumer data and consumers are concerned about how personal information is being used by marketers.

Several methods for obtaining consumer information were discussed in this chapter. These include information obtained as part of the marketing exchange process, through public databases or through electronic means. Each of these main sources of data consists of several specific means for obtaining personal information from consumers. The majority of information is collected through daily transactions, public databases and through electronic means, such as clickstream, cookies, software, and e-mail. More specifically, the marketing exchange process involves information obtained from sources that include interactive television and videotext, telephone's automatic number identification system, 0800 and 0900 numbers, automatic diallers CD-ROM's and secondary sources of information. Similar methods are used for collecting personal information of children and this raises consumer privacy concerns. Lack of consumer knowledge of such data collection and use is one of the major consumer privacy concerns that need to be addressed. Secrecy of data collection should be avoided by informing consumers of data collection and use practices. Consumer privacy concern will vary depending on the specific methods used to obtain consumer data.

Marketers have several uses for consumer information. Data from various sources are aggregated and then used to compile consumer data lists and databases. Data mining techniques are used to analyse such data and for identifying consumer wants and needs. The information enables marketers to segment consumer markets and for the development of targeted advertising messages and customised products and services. To conclude, such information improves the overall marketing strategy and results in more efficient marketing practice. The availability of consumer information are therefore of great importance to database marketing. Marketers will continuously attempt to obtain such data and use it in a meaningful way. Inappropriate use for consumer information however, raises consumer privacy concern. This may include the use of children' data, secondary use of consumer data and the use of consumer data for financial gain. Children's data are used in the same way as adults' data but it raises concern because third parties can obtain unauthorised access to data and children are unable to protect themselves against harmful activities from others. Database marketers do not consider data practices as an invasion of privacy, since they consider themselves owners of obtained data because they bear the costs associated with data collection, processing and storage. Therefore, database marketers argue they can do with the data whatever they want, including selling or renting such data. With regard to children's data, marketers claim that they cannot be held responsible to ensure children's privacy and safety, but rather, parents should be responsible to protect their children. The issues that raise consumer privacy concerns need to be addressed and preferably solutions need to be found to ensure sustainable database marketing practices in future.

Marketers do need consumer information for more effective marketing programs, but should acknowledge that consumers have certain privacy needs. Consumers' privacy concerns have implications for the regulation of database marketing activities. Database marketers prefer industry self-regulation as means for protecting consumer privacy. However, if consumers believe they do not have adequate levels of privacy it is most likely that government will impose legislation to protect consumer privacy, if consumers claim their privacy rights. Government regulation will restrict database marketing activities, which are currently essential for the development of effective marketing programs. Marketers should therefore not ignore the privacy concerns of consumers but should rather, address these issues to ensure a more balanced marketplace.

CHAPTER 4

CONSUMER PRIVACY CONCERNS RELATED TO DATABASE MARKETING PRACTICES

4.1 INTRODUCTION

Consumers sometimes perceive database marketing activities as a threat to personal privacy. Marketers' data practices that may raise privacy concerns mainly consist of data gathering, with subsequent data processing, storage, use and dissemination. Consumers may however also benefit from marketers' use of personal information. These concerns for privacy and the possible trade-offs warrant some consideration. Firstly, reference will be made to consumer differences on the issue of privacy. Secondly, consumer perspectives on database marketing activities, with specific reference to privacy concerns, will be discussed.

4.2 DIFFERENT CONSUMER PERSPECTIVES ON PRIVACY

Chapter 2 referred to McQuoid-Mason's definition of a consumer – any person who is affected by the use of goods or services, whether or not he or she bought, hired or used them. Also, Chapter 2 concluded that consumers have various levels of privacy concerns. The reasons being, consumers have different cultural backgrounds and not everyone is exposed to database marketing to the same extent. Other factors that may influence consumers' perspectives on privacy will be discussed in paragraph 4.3.8.

4.2.1 Consumer clusters

As far as privacy concerns go, consumers around the globe can be classified into clusters with more or less the same attitudes. Westin (Cespedes and Smith, 1993) distinguished among three groups of consumers in respect of information privacy: fundamentalists, unconcerned consumers and pragmatists. Research by Cranor, Reagle and Ackerman (1999) found similar results and proposed the following generally accepted clusters of consumers:

- Privacy fundamentalists – these are consumers who are extremely concerned about the use and dissemination of personal data and are generally unwilling to provide data when requested, even when privacy protection measures are in place. According to this study,

this group also felt quite often as if personal privacy was infringed, but this is most likely due to their sensitivity towards privacy issues.

- Pragmatists – consumers classified into this group were also concerned about data use and dissemination, but less than the fundamentalists. Mostly, pragmatists have very specific concerns and particular tactics for addressing them. Westin suggested that pragmatists weigh the benefits of various consumer opportunities and services against the degree of personal information sought (Cespedes and Smith, 1993).

- The marginally concerned – this group of consumers were generally willing to provide data when requested. However, under some conditions they did express a mild general concern about privacy.

4.2.2 The South African consumer

South Africa has similar characteristics as other third world developing countries, being one itself. A study in Argentina found that there are several factors, which can influence consumers' perception regarding database marketing activities and the invasion of consumer privacy (Milne, Beckman and Taubman, 1996: 23). The results of this study could be relevant to the South African context because Argentina is also a developing third world country. According to this study, consumers in different countries will vary regarding the concern for privacy to the extent that consumers are exposed to certain factors. Factors that have been identified in Argentina firstly include infrastructure, which were inadequate and secondly technological developments, which were in its infancy stage but was quickly improving. The influence of these factors on database marketing activities and the consequent consumer privacy concerns should be considered. Currently, consumers in both South Africa and Argentina are relatively unaware of database marketing practices and are therefore not as concerned about personal privacy like consumers in developed countries such as the United States of America and Europe. However, improvements in the database marketing infrastructure would most likely result in a strong growth in database marketing activities. An increase in such database marketing activity would raise more consumer privacy concerns. Likewise as technological advancements are implemented, consumers will become more knowledgeable of database marketing practices and this could raise the level of concern for privacy.

4.3 DATABASE MARKETING PRACTICES THAT RAISE CONSUMER PRIVACY CONCERN

The previous chapter referred to several database marketers' information collection and use activities. It also suggested that marketers need consumer information to improve their marketing strategy. The following sections will address these activities from the consumer's point of view. Several studies have been undertaken to determine factors, which are consistently important correlates of consumer privacy concerns. Consequently, various factors have been identified and these will be discussed in paragraphs 4.3.1 to 4.3.13. Phelps et al (2000) suggested however, that the primary drivers of consumer concern are the types of information collected and the amount of control consumers have over subsequent dissemination of data.

4.3.1 Consumer knowledge of data collection and use

The extent, to which consumers have knowledge of data collection and the subsequent use of such data, will determine what they perceive as an invasion of privacy. Consumers' knowledge of marketing practices typically falls into one of three categories (Nowak and Phelps, 1995: 52):

- Full knowledge of data collection and data use(s);
- Knowledge of collection but not of uses(s); and
- Ignorance of both collection and use(s).

It is assumed that consumers have knowledge of data collection if the data collection method employed was evident; it requires a priori consumer consent; the consumer willingly provided the requested information. If consumers were also made aware of all subsequent uses of the information, privacy would not have been an issue, from a legal, social, or ethical standpoint. In cases where consumers only provide personal information because the market exchange requires it, privacy concerns are alleviated by the voluntary nature of the transaction if consumers have had knowledge of information collection and use (Nowak and Phelps, 1995: 52).

There are two instances where the data collection and use practices of marketers are most likely to threaten consumer privacy. First, consumers have knowledge of collection and have given consent to information collection, but information is then used in ways consumers have

little or no knowledge of. Second, consumers lack knowledge of information collection and this took place without their consent, and consumers lack knowledge of how the information will be used (Nowak and Phelps, 1995: 52). The above-mentioned instances are summarised in Table 4.1.

TABLE 4.1: CONSUMERS' INFORMATION-RELATED KNOWLEDGE AND CONTROL

PRIVACY DOES NOT MATTER	**HIGH CONTROL, HIGH KNOWLEDGE** • Consumer willingly supplies the information to the marketer, for a specific purpose, which is known to the consumer. The marketer uses that information only for the purpose it was originally collected.
PRIVACY MAY MATTER UNLESS...	**MEDIUM CONTROL, MEDIUM-HIGH KNOWLEDGE** Privacy concerns are reduced by the following: • Consumers are made aware anytime individual-level information is being collected. • Marketers inform consumers of the uses of the information that consumers are asked to provide. • Consumers are allowed easy access to the information that pertains to them (e.g. allowing the consumer to check his or her credit rating information). • Marketers' allow consumers to "opt-off" lists, etc., that sold, traded, or rented to other marketers.
PRIVACY MATTERS	**LITTLE OR NO CONTROL, LOW KNOWLEDGE** • Consumers is unaware information is being collected and therefore unaware of the uses of that information. • Consumers supply the information for one purpose and the information is used for other purposes without the consumer's knowledge or consent. • A third party supplies individual-level information without the consumer's knowledge or consent to the data transfer or to the ultimate uses of that data.

Source: Nowak, G. J. & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: determining how and when "privacy" matters. Journal of Direct Marketing, 9(3), 57.

4.3.2 Individual-level versus group-level data

The use of consumer information to guide marketing and promotion efforts is not a new tendency. In the past marketers have relied on market-level information. Nowadays, individual-specific data are easy to access and to aggregate due to advances in computer technology and marketers therefore tend to prefer the use of this data. Market-level information is not the primary concern for consumer privacy issues, but rather consumers tend to focus privacy concern on the use of individual-specific data. The differences between these data types are quite obvious. Market or group-level data are consumer information that reflects the generalised characteristics of a consumer group or market segment. On the other hand, individual-specific or personal data includes data such as names, addresses, demographic characteristics, lifestyle interests, shopping preferences, and purchase histories

of specific-identifiable individuals. Consumers would like certain aspects of their lives to stay private but when marketers use data related to these aspects individually, could perceive personal privacy as being invaded. Consumers feel more vulnerable when database marketers are able to identify specific individuals, rather than treating individuals within a group context (Phelps et al, 2000). Consumers do not want marketers to know what kind of person they are, what they like or dislike or what they are doing at present. Thus, consumers are concerned about the use of individual-identifiable information, rather than the use of information within a group level context (Westin, 1967: 172).

4.3.3 Types of personal data

The level of consumer privacy concern will vary depending on the type of personal data collected and used. In the following subparagraphs reference will be made to specific sensitive and non-sensitive information types, as well as to public sources of data.

4.3.3.1 Sensitive data versus non-sensitive data

Phelps et al (2000) stated that most of the individual-specific consumer information used for marketing purposes can be arranged into the subsequent five broad categories: demographic characteristics, lifestyle characteristics, shopping/purchasing habits, financial data and personal identifiers (e.g., names, addresses). These categories each evoke different consumer privacy concerns depending on what type of information is involved.

Consumers typically distinguish between sensitive or not-so-sensitive data. The level of consumers' privacy concerns increase when sensitive data is collected and used. Typical sensitive data includes financial data, credit data, specific personal information such as sexual preferences, and medical information (Taylor et al, 1995: 39). Likewise, a study done by Phelps et al (2000) indicated that consumers perceive the above mentioned as sensitive data, and they added 'any personal identifiers' to the list. On the other hand, not-so-sensitive data may include demographic and lifestyle-related information.

Medical and financial data needs special consideration, since many consumers are concerned about the database marketing practices that involve such data. Where individuals provide information to a doctor, a merchant, or a bank, they expect that those professionals or companies will only use information for the sole purpose of providing the service requested.

Unfortunately, current practices, both offline and online, prevent this expectation of privacy (Berman and Mulligan, 1999). Online data practices, however, evoke higher privacy concerns and it has two pitfalls: unauthorised access to, and commercial use of sensitive medical and financial information. Online databases will not ensure the confidentiality of these records and third parties could gain access to these and the information can then be misused. Consumers do not want medical or financial information to be distributed for marketing purposes, except if information was voluntarily provided (FTC, 1996).

4.3.3.2 Public records

Nowak and Phelps (1992: 38) suggested that consumers are unaware that government entities' public records are used to obtain consumer information. Typical public data sources include data from birth certificates and vehicle registration forms. Consumers seem to be less concerned when data from public records are collected and used because of lack of knowledge of data collection and usage. Since much of the personal information used by database marketers came from public records, these practices should receive more attention. The use of these information types might result in higher privacy concerns when consumers have knowledge of the sources of such data. On the other hand, one could think that government databases would be more accurate than for example, third parties who sell database for financial gain. Therefore, consideration should first be given to most harmful practices until more important concerns rise (Nowak and Phelps, 1992: 38).

4.3.4 Volume of data collection and use

Consumers are becoming increasingly concerned about the amount and depth of information businesses and marketers collect about them (Hagel III and Rayport, 1997: 53). Consumers believe that excessive amounts of personal information are collected and that marketers rather should focus on information really needed for effective marketing programs (Nowak and Phelps, 1992: 37). In addition, consumers assume that marketers only use the information, which was provided voluntarily, but do not always realise the other data sources to which marketers have access (Taylor et al, 1995: 39). When realising this, consumers often feel helpless in their efforts to identify the means of acquisition, and the location of the information, or find themselves unable to correct inaccurate information and remove private information from databases (Morris and Pharr, 1992: 42). Consumers are becoming aware that the information they have given so freely through daily commercial transactions,

financial arrangements, and survey responses have value and that they receive very little in exchange for that value (Hagel III and Rayport, 1997: 53).

4.3.5 Individual and group pattern discovery

The level of consumers' privacy concern may vary depending on whether marketers use data for individual or group pattern discovery. Most privacy issues deals with basic storage and retrieval of personal data that precedes any knowledge discovery. Consumers are concerned about, for example, who can find out "What cereal person X bought on April 7, 1995?". When such information is collected, it is technically possible to find patterns such as how frequently person X buys cereal and what brand of cereal he or she prefers. Although this is just a simple example, consumers are concerned about discovered patterns in personal data that may involve controversial issues, such as race, religion, and sexual orientation. Sometimes, marketers use data to discover certain group patterns, which are reasonable to consumers. However, when these group patterns are combined in assessing the probability of likely consumer behaviour or responses, consumers may become offended, especially when small databases are used. Incorrect information could lead to misclassifications that could be seen as an invasion of privacy. Research indicated that people have been classified with having a probability of 0.9 to be infected by HIV, when no relevant ground existed for making such classification (Piatetsky-Shapiro, 1995).

4.3.6 Primary versus secondary information use

Consumers are less concerned about issues related to the primary use of information. Primary use of information involves "information collected, processed, or used to support sales, customer service, personnel, inventory, purchasing, or other applications in the context of an ongoing relationship established voluntarily between an organisation and its customers, employees, or suppliers". Consumers believe primary information use improves the exchange relationship between the company and oneself and that it is necessary to complete the transaction successfully (Culnan, 1993: 342).

Culnan (1993: 342) defined secondary information use as the "use of personal information for other purposes subsequent to the original transaction between an individual and an organisation when the information was collected". Secondary information is commonly used and legally accepted, but many perceive this as an invasion of privacy when it occurs without

the knowledge or implied or explicit consent of the consumer. Secondary use of information involves third parties who might gain access to personal data. Such third parties could range from the individual and the merchant in a cash transaction, to an affiliated issuer, transaction processor, credit card company or the individual who process the credit card transaction (Berman and Mulligan, 1999). Consumers believe it is wrong for companies to provide consumer lists to other entities and want to know the procedures to remove names from such lists (Phelps et al, 2000). Consumers would also like to limit access to personal data and want to have some control over subsequent information use (Nowak and Phelps, 1992: 37).

4.3.7 Inaccurate consumer databases

The existence of data errors is increasingly becoming a problem for consumers. These inaccurate data are often rented, sold or disseminated to third parties and it might become impossible to correct. The advances in technology should guarantee that the rate, volume, and detail of personal information captured would continue to increase dramatically. However, there are few assurances that these advances will not also dramatically increase the rate at which errors are introduced into this data. It is very difficult to completely eliminate inaccurate data because after such data sources have been cleaned it can be "re-infected" by other data sources which have not been up-dated yet (Privacy Inc's Consumer Privacy Guide, 1998).

4.3.8 The influence of consumer characteristics on privacy concerns

Several consumer characteristics may influence the level of concern regarding one's privacy. This may also determine in which consumer cluster group, as was discussed in paragraph 3.4.1.1, a consumer may be categorised.

4.3.8.1 Consumers' age

Nowak and Phelps (1992: 37) proposed that there is a difference between varying age groups' concern for privacy. It seems that consumers in the older age bracket have more concern for privacy, although they have a wider and more appropriate, perspective when judging marketers' information practices. Conversely, consumers in the younger age bracket are less concerned with privacy, but were more likely to have requested removal from mailing lists.

This implies that concern is reduced by the ability to take action or by having some control over the collection and use of one's personal information.

4.3.8.2 Consumer attitudes and shopping behaviour

Privacy concerns appear to be related to consumers' attitudes and shopping habits. The more favourable consumers' attitudes toward database marketing offers, which are a result of the database marketing process, the greater would the acceptance of such offers be (Phelps et al, 2000). Users of database marketing offers differ from nonusers in the concern for privacy of personal information. People using direct mail for purchasing have greater privacy concerns and would more likely have refused to provide personal information when requested, according to Westin's 1995 analysis of the 1994 Harris-Equifax data (Phelps et al, 2000).

4.3.8.3 Perception of good marketing ethics

Consumers' concern for privacy is often confused with concern for good marketing ethics because consumers are unable to distinguish between database marketing practices that appear to be unethical issues or whether it should be regarded as a privacy issue. When consumers attach ethics to a specific database marketing practice, marketers might get away with continuing such activities. Consumers tend to attach relatively less concern or consideration to poor ethical practices than to invasion of privacy issues (Taylor et al, 1995: 39).

4.3.9 Benefits in exchange for the provision of information

Many consumers claim that they are not always concerned about personal privacy but rather the fact that personal information is provided for free without being rewarded relatively to the cost reductions database marketers may receive. However, marketers believe consumers receive intangible benefits such as improved products and service and the availability of more product and service offerings. Thus, most consumers have shown a willingness to release personal information if they can benefit by doing so. A good example is the success of frequent-flier programs, which requires detailed information about consumers' flight histories in return for discounts on future flights (Hagel III and Rayport, 1997: 54-55).

Hagel III and Rayport (1997: 55) proposed that consumers are sometimes willing to pay premium prices for the customised products and services companies may deliver when using

personal information effectively. Often, consumers would react upon database marketing offers for reasons such as convenience, which results from saving time and effort. Consequently, consumers would probably be more willing to provide personal data when these benefits are present (Phelps et al, 2000).

4.3.10 Electronic monitoring

Information technology and the Internet created an exciting new marketplace for consumers. It offers easy access to a broad range of goods, services, and information, but also serves as a source for database marketers of vast amounts of personal information about consumers, including children. While the online consumer market is growing exponentially, there are also indications that consumers are cautious when participating in it because of concerns about how personal information are being monitored and used (FTC, 1998a).

The Privacy for Consumers and Workers Act of the United States of America (Taylor et al, 1995: 40) defined electronic monitoring as "the collection, storage, analysis, and reporting of information concerning an individual's activities by means of a computer, electronic observation and supervision, remote telephone call accounting, or other form of visual, auditory, or computer-based surveillance conducted by any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system".

Consumers have less confidence in how online service providers and merchants use personal information in comparison with traditionally offline institutions, such as hospitals and banks, use such information (FTC: 1998a). New database technologies enable online profiling and make the development of databases, through the combination of data from a variety of sources, possible (Steer, 1999). Information technology facilitates the free flow of data and will become difficult to maintain because the privacy rights of individuals and businesses will continue to be challenged from many new directions (Grover, et al, 1998: 5). A study done by Cranor (2000) also identified several other consumer concerns regarding online privacy. First is the issue of high distrust that exists regardless of the type of electronic-commerce site visited. Second, consumers are concerned about staying anonymous when going online. They are willing to share opinions anonymously, but most are unwilling to share information, which can be traced back to the individual. Third, consumers are concerned about automatic data transfer. Fourth, privacy concerns result from data, which is often collected without

knowledge (Cranor, 2000). Electronic means allow easy, cheap and automatic collection of data without meaningful choice given to individuals. The last online concern is that of data, which can be obtained and merged from many sources and therefore even non-identifiable data can become identified. All the above, mentioned concerns' relevance was supported by findings of the April 1997 Louis Harris Poll of Internet users (Cranor, 2000).

Dentino (1994: 38) developed the following formulation that suggests information technology violates consumer privacy:

Technology + information + no restraint = violation.

Advancements in data-processing technology enable marketers to access and manipulate data better, smarter, faster and cheaper than ever before. If one combines this with the availability of a vast amount of information and lastly, add to the mix, the fact that there is basically no restraint over how consumer information is used…the result would be a recipe for privacy violation if you were not careful (Dentino, 1994: 39).

The Internet with its possibility of electronic monitoring is an important marketing tool for collecting information for database marketing purposes, more so than traditional methods used for obtaining consumer data. The use of electronic means for collecting consumer data however, raise important privacy concerns, especially due to the secrecy of information collection and the vast amounts of personal information collected. Consumers would like to limit the electronic monitoring of online activities and have more control over the collection and use of personal information. Available options for protecting consumer privacy will be discussed in Chapter 5.

4.3.11 Collection and use of children's information

Another important consumer privacy concern relates to the online monitoring of children while browsing the Internet. As mentioned previously, the Internet is an important tool for database marketers in obtaining and for disseminating consumer data, and this is also applicable to children's data. Children represent a rapidly growing segment of online consumers and therefore it is important for database marketers to compile extensive databases from children. Children's databases are used for a variety of purposes that often raise privacy concerns (FTC, 1998a). Concerns include children who do not understand the impact of the

information provided to advertisers or that the "game" played is just for the purpose of data collection. Children lack the developmental ability to distinguish between marketing and entertainment activities (Austin and Reed, 1999: 591).

Database marketers use kids' clubs to generate brand loyalty for products offered. However, parents may not be aware when children gain access to the Internet and what personal information about themselves and their parents, has been provided to a company. In addition, some kids' clubs use inappropriate ways to gain information for database marketing purposes and no value is offered in exchange. Indeed there is certain sites such as http://www.barbie.com that advise children to get their parent's permission to use the Web site and which demand parents to type in the child's user name and a parental password before access will be granted (Austin and Reed, 1999: 595).

Unauthorised access to children's databases may result in third parties that target children with inappropriate content or offensive product and service offerings. Unwanted exposure to such material is seen as an invasion of consumer or children's privacy (Austin and Reed, 1999: 595). There are few, if any, control mechanisms to protect children's data from unauthorised access by database marketers or other third parties. Many have identified the wrongful use of children's information and authorities need to regulate these uses (O'Leary, 1995).

The last concern is related to databases that enable marketing practices such as one-to-one marketing. For example, instead of doing a television commercial that is roughly aimed at boys between five to seven, you are targeting a particular boy online who has particular interests. It is now possible to ask the child "Bob, wouldn't you like to have this new action figure, just like you saw in the movie last week?" At this level of targeting, the opportunity for manipulation becomes much greater, and parents have less control over their children. All these practices need to change, in order to alleviate parents' growing concern about children's privacy (Austin and Reed, 1999: 597).

4.3.12 Prosser's legal torts

Many consumers claim that database marketing practices intrude upon personal privacy. However, Prosser's framework suggests, that from a legal perspective, only disclosure and to a lesser extend appropriation, could be considered as relevant to consumer privacy concerns. These database marketing practices often evoke two perceptions people have: annoyance and

violation. Annoyance results, for example, from receiving too much database marketing offers, such as direct mail and too many telemarketing solicitations. Violation because individuals feel that too much information about their lives and personal preferences is being exchanged without having knowledge or given consent. Irrelevance of such marketing offers aggravates these concerns. Consumers argue that marketers should consider the relevance of products and services before targeting them with such offers. Marketers argue that as the use of databases increase, the volume of irrelevant mail and phone calls will decline (Dentino, 1994: 38).

4.3.13 Business-to-business marketing

The issue of privacy is not exclusive to marketers of consumer goods. Privacy is also increasingly emerging as a major business-to-business marketing issue. Business-to-business marketers need to be equally proactive on the privacy front as consumer marketers do. Though business information is less personally sensitive, the general heightened feeling of concern, still exist (Loro, 1998: 17). Businesspeople want to know how information is being collected, if it is secure, and if other less legitimate companies could gain access to the data. Business marketers mainly use data to classify business into homogeneous groups of potential business customers, based on characteristics of the businesses (Loro, 1998: 24).

4.4 BALANCING CONSUMERS' PRIVACY CONCERNS AND MARKETERS' INFORMATION NEEDS

Ideally, the balance of power between consumers and marketers should be more or less equal, but the marketplace is imperfect. If the power balance changes dramatically to either side, one party might be threatened (Froomkin, 1996). Power balances may result from any of the parties having too much control over the other. For example, if consumers' privacy rights are being threatened by marketers' information practices and nothing is being done to equalise the balance, consumers might feel they have little or no control and therefore the balance would be in marketers' hands. On the other hand, if strict policies and legislation that could have resulted from consumer complaints were regulating marketers' practices, the balance would be in consumers' hands. It is very important to determine an acceptable solution for both parties involved. According to Taylor et al (1995: 45), both consumers and marketing practitioners believe that law and business practices are not adequately protecting privacy rights and are convinced that something needs changing.

When addressing consumer privacy concerns it would simply not be enough to use the individual's "right to be left alone", as privacy advocates typically do, or a company's "information property rights", as managers often do, as separate viewpoints. Rather than being left alone, most people wants protection against negligent uses of personal information but without a decrease in product choice and consumer flexibility. Similarly, no company wants to alienate potential customers by database marketing efforts, but rather, wants access to relevant consumer data so products and marketing programs can respond to dynamic changes in consumer demand (Cespedes and Smith, 1993: 8-9).

4.4.1 Privacy within a social context

Consumers do not desire a complete state of privacy, but privacy has a social utility, which can advance the goals of the entire society. Privacy should therefore be considered as a means to an end, where privacy forms the basis for a democratic nation (The protection of privacy, 2000). In any liberal society privacy is essential for free and unrestricted communication. The exchange of ideas and information requires persons to express themselves at all levels in the society without fear that one's remarks will become public property or should be used to infringe upon privacy. If perfect judgement has been possible there would be no reason to fear unauthorised disclosure. However, since this is impossible, the need for confidential exchanges will remain. Society will benefit to the extent that information exchanged confidentially is more accurate. This must be taken into account when developing protection measures for privacy (Moore, 1984: 76).

The protection of values, which is fundamental across cultures, is essential to ensure a more balanced society. Examples of such values are freedom of speech, the right to personal freedom, and the right to informed consent. Individual privacy is at the core of many of these basic, minimal rights. Accordingly, it would appear that the value of privacy to civilised society is as great as the value of the various fundamental rights to civil existence (Pincus and Johns, 1997: 1238).

4.4.2 Trade-offs between consumer privacy concerns and marketer information needs

Marketers and consumers are concerned about the intended use of consumer information, but tend to focus on different aspects of information privacy (Briefly noted, 1997). There are

several trade-offs associated with marketing practices and consumer privacy concerns that warrant discussion here.

4.4.2.1 Individual-level versus group-level data

Ziarko (1995) made the following comments regarding the use of both individual-level and group-level data. It is very difficult and costly to acquire new knowledge by using individual databases, unless many are linked together. Marketers are more interested in using aggregated group data for new knowledge discovery activities. The aim is to identify groups of people that may be interested in buying products or services, rather than being preoccupied or inquiring about the individual consumer. Therefore, consumers need not be concerned about the use of individual-level data because knowledge about groups is generally used to guide decisions affecting individuals.

4.4.2.2 Types of information

The types of information collected and used by marketers have several implications for consumer privacy concerns. Consumers' greatest concern is when financial, medical and personal identifier information is collected and used. Database marketers should determine the relevance of such information for marketing practices. The use of timely and relevant information could balance consumer concerns with legitimate business needs for information. On the other hand, consumers do not object when demographic or lifestyle-related information is requested. Therefore, the reduction in use of these information types will do little to alleviate privacy concerns. Database marketers should rather limit the collection and use of sensitive information types to alleviate consumers' privacy concerns and should concentrate on collecting only consumer information relevant for the specific marketing purpose (Phelps et al, 2000).

4.4.2.3 Knowledge of data collection and use

Consumers would like to be more informed about database marketers' use of personal information. Database marketers will benefit from more informed consumers because consumers tend to be less concerned about privacy when having knowledge of information practices. The mere fact that marketers seem concerned about consumer privacy would probably alleviate privacy concerns. Therefore, database marketers could educate consumers

on how information is gathered, used, stored and shared because this would reduce misunderstanding and will alleviate privacy concerns (Phelps et al, 2000).

4.4.2.4 Information control

Most consumers desire more control over personal information. Marketers perceive this as a limitation when compiling detailed databases and fear an increase in data acquisition costs. However, marketers should make some compromises and provide for consumer access to databases and lists. Although only a small fraction of consumers would use the opportunity to opt-out of the use of personal information, it is important that the opportunity exists. Offering more control over information has a relatively dramatic impact on consumers' purchase intentions and consumers are more receptive of, and interested in advertising offers that was partly initiated by them. Related to information control are consumers' concerns about the large amount of, for example, catalogues and advertising mail received. Consumers believe that more control over personal information will result in less unwanted mail and telephone solicitations (Phelps et al, 2000).

On the other hand, marketers may not want to reduce advertising volume because marketers believe that the marketing message may get lost in the clutter of competitive promotions. However, it would benefit database marketers, if the volume of marketing offers, are reduced especially if consumers are overwhelmed with these offers. Database marketers also need to increase the relevance of marketing offers. This could be accomplished by greater efficiencies in the use of personal information and database technology (Phelps et al, 2000).

4.4.2.5 Costs and benefits of information exchange

Currently, consumers receive several benefits from apparent inherent efficiencies of marketers' micro-segmentation efforts. These should not be ignored when determining a model for protecting consumer privacy. Greater efficiency in determining consumer wants and needs could result in products that offer greater consumer satisfaction at more reasonable prices. Consumers, would probably also have greater awareness of goods and services available for particular lifestyles. However, to receive such benefits involve certain direct and indirect costs. Costs are associated with less privacy when consumer information is collected, aggregated and shared amongst different databases for profit and non-profit purposes (Morris and Pharr, 1992: 31).

At the other extreme side of the privacy continuum, the consumer would be in control of personal information, which is used by marketers. Consumers want to control the storage, retrieval, dissemination, use, and content of information others maintain or have access to. The costs would be associated with negative effects on marketing efficiencies. This could for example lead to less satisfying products with increased prices. Thus, all parties have a stake in the outcome of the debate on privacy. The balance is likely to be achieved by an acceptable sacrifice of privacy for consumer benefits such as awareness, product choice and cost (Morris and Pharr, 1992: 31).

4.4.2.6 Electronic monitoring and children's privacy issues

Advancements in database technology and the possible monitoring of individuals on the Internet could invade consumer privacy rights. The Internet does not create new privacy issues but rather, it makes the existing ones, like confidentiality, legitimacy and integrity of the personal information and the dissemination of information, difficult to control and secure. Database marketers use electronic means the same way as traditional means for data collection and use, but to a far greater extent. Consumers are therefore more concerned about newer methods for data collection and use (Akdeniz, 2000: 55).

4.4.2.7 Trust

An important factor that could possibly alleviate privacy concern is trust. When a trust relationship exist, consumers would be more likely to believe that information is used effectively and for ways that were intended. A database could be a tool-kit that facilitates consumer loyalty if used appropriately (Milne et al, 1996: 28). However, it is important to note that trust and loyalty can only be established over a long period of time (Rosenfield, 1996: 40).

4.4.3 Addressing privacy concerns

The successful outcome of the privacy debate depends on marketers' understanding of the relevant consumer issues and the ability to manage database marketing activities accordingly (Petrison and Wang, 1995: 20). The DMA of the United States of America has identified consumer privacy concern as the most important issue facing database marketers today and it threatens the very foundations of database marketing. These threats are most evident in the

form of regulatory legislation (Phelps, Gonzenbach and Johnson, 1994: 10). Legislation would typically result in marketers' losing the ability to use consumer information. Consequently, this would likely result in much higher levels of uncertainty faced by database marketers and marketing successes would then become less frequent and more costly. Database marketers should therefore acknowledge the very importance of addressing consumers' privacy concerns in attempting to achieve a more desirable balance in which to operate (Morris and Pharr, 1992: 31). Hence, the challenge in the business community is to make the most of the opportunities presented by the growth in information and database technology while, at the same time, protecting what remains of individual privacy (Pincus and Johns, 1997: 1237). Cespedes and Smith (1993) proposed several rules to which database marketers could adhere and which could serve as a starting point for demonstrating concern for consumer privacy issues and for protecting consumer privacy. These will be discussed in the following section.

4.5 RULES FOR REGULATING MARKETING INFORMATION PRACTICES

Principles and rules need to be implemented to ensure that appropriate levels of consumer privacy exist. Consumers perceive companies that comply with these rules, as being concerned about personal privacy and the result would typically be trust in a company's information practices. Trust has always been an important element of good marketing. It is therefore important to maintain a trust relationship especially with respect to database marketers' ability to keep personal information in the hands of those who have the consumer's consent, and to use that information in a fair and appropriate manner (Cespedes and Smith, 1993: 15).

In addition to the principles developed for alleviating consumers concern and building a trust relationship, which will be discussed in Chapter 5, Cespedes and Smith (1993: 15) developed a series of rules for addressing consumers' concerns and for establishing fair database marketing practices. Four general areas of consumer concern have been addressed by these rules and will be discussed in the following paragraphs.

4.5.1 Collection

In general, all data collection should operate according to a so-called "sunshine principle", where all the collection practices are disclosed to avoid scrutiny of consumers. Therefore,

Cespedes and Smith (1993: 15) proposed the following rule regarding the collection of personal information:

"Data users must have the clear consent of the data subject to use personal data for database marketing purposes".

Companies should explain both primary and secondary uses for data to individuals before they give consent for collection, because this would limit later charges of improper information practices. Data collected through deceptive means could backlash. Therefore, Cespedes and Smith (1993: 16) suggested that companies should avoid deception and secrecy in data collection and proposed the following consequences to the rule regarding data collection.

Corollary A: "Secretive collection itself and not knowing what information is being collected, makes consumers suspicious and raises concerns".

Corollary B: "Targeted consumers should know the marketer's source for information about them".

Corollary C: "Individuals should have the opportunity to opt out of subsequent uses of data". Companies should only be allowed to use data for subsequent purposes if consumers' consent has been given for each use (Cespedes and Smith, 1993: 16).

Cross-referencing is another area of consumer concern that relates to the sharing and dissemination of data to third parties. Relevant to cross-referencing, the fourth corollary regarding the data collection rule can be assumed. It suggests that consumers' consent should be granted before data are shared with third parties.

Corollary D: "A consumer's consent to data use by one company does not automatically transfer to companies sharing that information".

The compilation of consumer data from multiple sources provides marketers with a strategic advantage when formulating marketing programs. However, it is important to explain to consumers the intended uses of the collected data and to provide for the option to opt-out of secondary data uses that consumers may find unacceptable. Therefore, although nothing is inherently wrong with secondary or cross-referenced use of information, marketers still need to inform consumers of these information uses (Cespedes and Smith, 1993: 17-18).

4.5.2 Data management

Effective database marketing can reduce advertising clutter and other marketing-related issues by targeting consumers most interested in the specific products and services. However, poor data management practices may prevent this from happening. Many consumer databases are not being maintained or updated on a regular basis and consequently its use will decrease over time (Cespedes and Smith, 1993: 18). Therefore, a second rule related to management practices is suggested:

"Companies are responsible for the accuracy of the data they use, and the data subjects should have the right to access, verify, and change information about themselves".

An improvement in data management will most likely result in improved data accuracy and this will enable better targeting. Data processing and storage needs to be handled with care and the database marketing infrastructure's efficiency should be increased (Cespedes and Smith, 1993: 18).

4.5.3 Categorisation

Cespedes and Smith (1993: 18-19) stated that after data have been collected and cross-referenced, it usually should be categorised or segmented according to homogeneous consumer groups. Marketers argue that individuals who differ in terms of demographics, attitudes, or life circumstances are likely to purchase in different ways. Conversely, consumers with similar characteristics are assumed to have similar buying patterns. Marketers also recognise the implication of this social diversity for product and service development. However, to ensure fair information practices Cespedes and Smith (1993: 19) proposed a third rule, which stated:

"Categorisations should be based on actual behaviour as well as the more traditional criteria of attitudes, lifestyles, and demographics".

There is little theoretical or empirical support for marketers' view that consumers can be grouped into segments, which can actually predict consumer behaviour. Consumers feel offended when marketers consider some facts about them and then attach a certain profile to them. This rule could therefore alleviate these concerns. Consumer classifications would be more accurate when based on actual purchase behaviour and attitudinal data that can help to explain behaviour. Otherwise, the result can be inaccurate conclusions about current or potential customers that raise privacy concerns, and could lead to a loss of potential effective marketing opportunities (Cespedes and Smith, 1993: 19).

4.5.4 Implementation of rules regarding data collection and use

The implementation of the proposed rules requires specific actions from several groups: the companies employing database marketing activities, industry organisations, and legislature. First, companies using database marketing could audit current and future programs to determine if practices comply with these rules. Second, industry groups should also play a more active role. Industry groups could find ways of applying visible marketplace pressures for compliance and could even publicise bad practices. Finally, legislature could put effort into educating themselves, consumers and marketers about the risks and benefits of database marketing practices. When considering potential legislation, one should remember that, if database marketing is used properly, it could result in improved efficiencies for both marketers and consumers. Smaller companies might also benefit from having access to data already available to most large corporations. However, insufficient self-regulatory practices would make additional regulation inevitable (Cespedes and Smith, 1993: 19-20).

Privacy advocates should recognise that incorporating the proposed rules and principles do not mean an "erosion" of personal privacy. Rather, it means more informed consumers and it would most likely alleviate consumer privacy concerns. Conversely, marketers should recognise that the rules, although having cost implications, do not mean an end to database marketing. Rather, it means an end to bad database marketing practices that could have resulted in restrictive legislation and in addition, that marketers could benefit from better and more accurate consumer information (Cespedes and Smith, 1993: 20).

4.6 SUMMARY AND IMPLICATIONS FOR DATABASE MARKETING

Database marketing activities that involve the collection and use of consumer information, raises several consumer privacy concerns. One can distinguish between several consumer clusters depending on consumers' attitudes on database marketing practices and personal privacy. The typical South African consumer is classified as a "pragmatist". Pragmatists are concerned with privacy to the extent they are exposed to database marketing activities. The South African database marketing industry is still in its infancy phase and as the industry progresses, and consumers become more knowledgeable, privacy concerns would also increase.

The primary driver of consumer concern is the general lack of knowledge on data collection and use. When consumers have full knowledge of data collection and use, there would be no privacy issue involved. However, when consumers have knowledge of collection but not of subsequent use, or they lack knowledge of both data collection and use, it raises privacy concerns. Database marketers could alleviate this concern by disclosing data collection and use practices. Consumers will be more informed about data practices and therefore will better know how to protect themselves. If consumers are able to protect themselves, by for example having knowledge of an opt-out system and using such an opportunity, consumers will be able to enhance personal privacy, which in turn could alleviate privacy concerns. Privacy concerns also relates to the type of information collected and the amount of control consumers have over subsequent use of data. Other factors that raise consumer concerns include: the use of personal information to identify specific individuals; collection and use of sensitive information, such as medical and financial data, rather than the collection of demographic and lifestyle data; the volume of information collected and used; secondary information use; the use and dissemination of inaccurate databases; the collection and use of children's data and the lack of benefits received in exchange for information provided. Consumers have also expressed a concern for online database marketing practices because of the secrecy in data collection and use. However, concerns may vary depending on consumers' cultural orientation, age, perception on what constitutes good marketing ethics or the specific methods employed to obtain consumer data.

Data practices may evoke consumer privacy concern, but it is important to note that database marketing activities may hold many benefits for consumers. Improved products and services, and a greater variety of products and services available to the consumer are likely to result from better market research. Consumer information solely used for marketing purposes and to enhance the marketing exchange process is therefore generally not seen as a major consumer concern. Consumers need to be made aware of all the benefits to make an informed choice on whether to provide information or not, and on whether privacy is really being threatened by database marketing practices. Consumers are generally not concerned with the collection and use of personal information when they have given explicit consent or when providing information voluntarily.

Marketers' information needs and consumers' privacy needs should somehow be balanced in order to withhold strict government intervention. Absolute privacy is not the important social goal but consumers expect a reasonable level of privacy. Awareness of trade-offs between

marketers' and consumers' needs should be established through business and consumer education. Compromises from both sides are necessary to reach a more balanced relationship between the two parties. The successful outcome of the privacy debate will depend on marketers' understanding of consumer concerns and by addressing these concerns accordingly. Several rules have been proposed to serve as a starting point for database marketers to demonstrate concern for the issue of consumer privacy. These need to be implemented to ensure sustainable database marketing efforts.

CHAPTER 5

APPROACHES AND MODELS FOR REGULATING DATABASE MARKETING PRACTICES

5.1 INTRODUCTION

The concept of privacy is not only hard to define, but it is also difficult to identify appropriate measures to ensure adequate levels of privacy. The mechanisms that are used to enhance consumer privacy are constrained by the need for information disclosure. Trade-offs between consumers' privacy needs and marketers' information needs are necessary to create a more adequate level of privacy, while ensuring effective marketing practice. A situation exists where the data collector and the data subject are two different principals, which both have a legitimate interest in the data but have different goals concerning its use.

Current approaches for regulating database marketing practices include privacy-enhancing information technologies, self-regulation and law enforcement. These approaches provide for different levels of consumer privacy. Policy makers must consider the unique characteristics of its country's database marketing industry and consumer types when determining which approach to follow (FTC, 1996). Several models have been proposed to identify combinations of the mentioned approaches for the protection of consumer privacy in different countries, and another model was developed to establish, to what extend a country's approach offers privacy protection. These approaches, together with the models, are discussed in this chapter.

5.2 PRIVACY-ENHANCING INFORMATION TECHNOLOGY

Information technology is frequently used for data collection and use purposes and these raise consumer privacy concerns. It can, however, when used constructively, improve an individual's control over the collection and use of personal information. Advances in information technology often address consumer privacy concerns. It is worth mentioning that the majority of information technologies have been developed to address online database marketing-related privacy concerns, rather than more traditional database marketing tools, which is used for data collection, processing and storage. Marc Rotenberg (Executive summary report: Proceedings to the industry Canada's symposium on privacy-enhancing

technologies, 1996: 7), the General Director of the Electronic Privacy Information Centre (EPIC) defined a privacy-enhancing technology as "one that eliminates the collection of personal information and where it is possible, hides the actual identity". Cranor stated (1996: 1) the value of information technology lies in its ability to accomplish the following in order to enhance consumer privacy:

- Facilitate the exchange of information regarding data collectors' information practices as well as individuals' privacy preferences;
- Makes automatic monitoring of data collectors' information practices possible;
- Enable secure transactions, while minimising the exchange of personal information;
- Protect private communication from interception and databases from being shared; and
- Permit individuals to control messages they may obtain through the Internet.

Information technology applied alone cannot solve all the problems related to consumer privacy. It is, however, a very good supplement for other privacy protection initiatives and in the long run it would be best to use it as such according to Morris and Pharr (1992: 42).

Several information technological means exist for protecting consumer privacy and to alleviate consumer concerns. Advances in information technology can be applied in both traditional database marketing tools such as the television and telephone, and to newer database marketing tools such as online targeting of consumers.

5.2.1 Privacy-enhancing information technology applied to database marketing

There are several information technology tools available that could be applied to enhance consumer privacy. Information technology tools, however, are mainly concerned with protecting consumer privacy where online database marketing activities are concerned. Privacy-enhancing information technology could therefore be seen as a tool for regulating fast changing information technology that actually raises consumer privacy concerns. Reference will be made in the next paragraph on the working and effectiveness of currently available privacy-enhancing information technology tools.

5.2.1.1 Filtering technologies

Filtering technology is probably one of the best-known information technology tools for protecting consumer privacy within the online database marketing environment. It allows for more control over the kind of information one gets exposed to over the Internet and therefore enhance consumers' ability to protect their own privacy. Child protection software is an example of filtering technology. A specific example of child protection software is the Platform for Internet Content Selection (PICS). It was developed to classify and label Internet sites on the basis of its content, by using certain standards. Consumers identify keywords of phrases related to the content they do not want to be exposed to, for example "violence". Software that picks up the classification ratings for each site could then block sites that obtain such material or it could only permit access to sites with specific ratings such as "academic libraries". This software is especially useful to parents because it enables the blocking of children's access to offensive or objectionable sites (FTC, 1996). PICS technology can be further extended to allow more sophisticated notice and choice options. A standard format is necessary for setting preferences such as "no transfers to third parties" on your computer software. The browser will match the consumer's preferences with regard to online marketers' data practices with the actual Web site's data practices. If the data practices are objectionable when comparing with consumer preferences, a warning sign will appear. Hence, consumers obtain more control over the collection and subsequent use of personal information. Software programs provide reasonable levels of information privacy, but responsibility for privacy protection is in consumers' hands (FTC, 1996).

5.2.1.2 Cookies

Cookies were also identified as a means for collecting personal information, and consequently raise consumer privacy concern. However, cookie technology can be applied to enhance consumer privacy. When used constructively it could be used to communicate a consumer's privacy preferences to a Web site. A consumer's privacy preferences refer to database marketing practices, which are acceptable to a particular online consumer. Privacy preferences are for example that a consumer does not want to visit sites that held third party cookies or that disseminates information to third parties. Once a consumer conveys his or her privacy preferences to a Web site or database marketer, the information could be stored. The consumer could then be treated online according to the specified privacy preferences (FTC, 1996).

5.2.1.3 Encryption

Encryption allows the transformation of data into a form that cannot be read by anyone who does not have access to the same decryption code or key as the sender. Therefore, it provides the means of "locking" and "unlocking" information so that only intended parties could gain access to it (Cavoukian, 1998: 187). The encryptors translate the data transmissions into a code that can only be understood by using the appropriate decryptor. Consumers may use encryption to guarantee the privacy of credit card information when buying online. Encryption is commonly used within business-to-business marketers, but a more convenient and easy accessible version is needed in order to succeed in the online consumer market (Leonard, 1996).

5.2.1.4 E-mail technology

Consumers' concerns regarding the receiving of unsolicited e-mail are being addressed by information technologies that sort incoming e-mail according to the sender, placing the e-mail from unknown senders, such as database marketers, in a low priority mailbox. Software could be programmed to identify unwanted messages by for example, looking for messages similar to those in a database of known junk mail. The individual can decide whether or not to read the message in the low priority mailbox. However, there are still a chance that individuals ignore e-mail messages that came from personal acquaintances such as long lost friends or colleagues. The system could otherwise be expanded to offer small incentives or electronic payments for reading e-mail messages. If the message was from someone the individual wishes to correspond with, he could ignore the payment. Otherwise, one could keep the payment to compensate for spending time reading the message. Individuals could also subscribe to junk mail filtering services, although until recently it has not been so accurate but will probably improve in the near future (Cranor, 1996).

Encryption, which was discussed in Paragraph 5.2.1.3, could also be applied to enhance consumers' privacy with regard to the receiving of unsolicited e-mail from database marketers. The availability of e-mail cryptographic tools, enable users to send anonymous electronic messages. Remailing programs are used to route a message through a series of remailers, and if properly implemented, cannot be traced back to its sender – not by either the remailer operator or by the recipient of the message. Remailing programs delete all identifying information about incoming e-mails and substitute a prior determined header.

Consumers may use encrypted e-mail to ensure communication with others remain private. Hence, database marketers cannot get hold of such information (Froomkin, 1996).

5.2.1.5 Current information technology research projects

Consumers could make use of specific agencies or entities to enhance information privacy when buying online. Research of such entities includes the Platform of Privacy Preferences, which will be briefly discussed in the following section.

Some companies designed a new protocol named Open Profiling Standard (OPS). The OPS enables online consumers to provide information only once and then it is stored in the Web browser. Hence, one do not have to re-enter one's information, such as one's name and address each time one purchase a product or register at a site (Coyle, 1998). A project initiated by the World Wide Web Consortium, the "Platform of Privacy Preferences" (P3P) was based on the OPS and provides a framework for online interactions. Once completed, the project will enable database marketers based on Web sites, to articulate data practices to consumers, for example which data are collected; what use the data have; and whether data are shared with third parties. These practices are made available in machine-readable format that could automatically be detected by Web browsers and compared with online consumers' privacy preferences, which are stored on the browser. If a match is found between the data practices and the consumers' preferences for data practices, a P3P agreement is reached. If no match was found, the browser would without delay, send a notice of the non-agreement. This typically occurs when encountering Web sites that employ objectionable data practices. Cranor (1998), one of the designers of P3P's, has also indicated that P3P includes a user data storage area for information consumers do not mind sharing with online database marketers. P3P can also facilitate choice by allowing Web sites to offer visitors a selection of privacy policies concerning data practices and it is up to the consumer to decide which policies are acceptable and whether to provide information to a specific Web site. However, P3P does not guarantee that mutually acceptable terms will always be found (Cranor, 1998).

5.2.1.6 Universal registration systems

Universal registration systems on the Internet allow both online consumers and Web sites to register with them. This system operates as follow: registration requires the provision of a selection of personal information to the system owner. In return, the consumer will receive an

identifier, which allows anonymous browsing of Web sites registered as part of the particular system. The sites visited are recorded as a non-identifiable entity and therefore the consumer remains anonymous and one's identity would not be revealed. The system owner will use the anonymous information within an individual-level and/or group-level context for purposes such as market research (FTC, 1996).

This system allows anonymous browsing by online consumers when visiting sites that are part of the specific universal registration system. At the same time it allows registered online database marketers to analyse site usage and aggregate consumer preferences. However, the disadvantage of a universal registration system is that it is restricted to registered consumers and database marketers and therefore would not ensure adequate protection to the majority of online consumers' privacy. The effectiveness of such a system depends on online database marketers' willingness to use non-identifiable data for database marketing purposes. Yet another limiting factor is the possible lack of knowledge of the existence and implementation of this system.

5.2.1.7 Anonymity and pseudonymity tools

Anonymity and pseudonymity tools also provide for more consumer control over marketers' data practices. These tools presume consumers can protect themselves against marketers' collection and use practices by browsing the Web anonymously. Available technology, which enables anonymous browsing, are for example anonymizing proxies and crowds. These will be discussed in the following two paragraphs.

Anonymizing proxies act as substitutes or alternatives for consumers when buying online. It submits requests to Web sites on behalf of consumers and therefore information about the consumer cannot be revealed. One of the well-known anonymity tools is the Anonymizer. However, this tool cannot protect an individual against Internet service providers logging into one's Web activities. For example, if one wants to request about travel destinations, but do not want one's information to be collected one can use an anonymizing proxy to submit the request on one's behalf (Cranor, 1998).

"Crowds" are based on the assumption that consumers could be anonymous when blending into a group. It is possible for online consumers who are geographically distributed, to join a group called a "crowd". This would enable group members to forward all HTTP requests

through the group without being identified individually. Each request is randomly forwarded to another crowd member, who can then either submit it directly to the end server or forward it to another crowd member. It is not possible for anyone that operates within the crowd or outside the crowd, such as the Web server, to identify where the requests have originated. This could be applied within the database marketing context where online consumers join a consumer crowd for sending requests for products or services offerings (Cranor, 1998).

5.2.2 Concluding remarks on privacy-enhancing information technology

There exist a variety of privacy-enhancing information technologies, which could be implemented to safeguard personal privacy and to alleviate consumers' privacy concerns. These technologies are mainly used to minimise the disclosure of personal information and to empower individuals to control the amount of personal information collected and used. However, privacy-enhancing information technology cannot be used as a single medium to protect consumers' privacy, but rather it is an adequate supplement to industry self-regulation and legislation protection efforts. A strong industry-wide and consumer commitment is necessary to ensure the adoption and use of privacy-enhancing information technologies.

5.3 INDUSTRY SELF-REGULATION

Self-regulation as means for enhancing consumer privacy has been proposed and supported by many industry organisations. Self-regulation within the consumer privacy context requires industry members to monitor own data practices and to ensure adequate levels of consumer privacy. Normally, database marketers adhere to implicit and explicit norms or ethics inherent to the specific industry and/or country in which database marketers operate. Several surveys and studies across industries have been done to identify widely accepted principles regarding the collection, use and dissemination of personal information. Direct Marketing Associations worldwide have provided broad guidelines to which members should adhere and have since the 1960's employed several self-regulation principles. Such principles have especially been adopted in the United States of America, Canada and Europe because the database marketing practices in these countries have progressed to an advanced level and therefore required more control over such practices (FTC, 2000). The database marketing industry of South Africa supports the accepted world standards regarding the use and dissemination of personal information. Nevertheless, the database marketing industry indicated that most, but not all of these principles have been included in the Open Democracy

Bill and industry members would like it to be entrenched in both the Open Democracy Act and in South African self-regulatory codes (DMA: The privacy file, 1998).

5.3.1 The South African database marketing industry

The DMA of South Africa was established in 1974 as a non-profit body representing over 400 local and international organisations involved in direct marketing and which make use of database marketing efforts (DMA: About the DMA, 2000). Members include private and governmental organisations involved in marketing practices by means of mail, telephone, television, radio, magazines and newspapers, fax, electronic mail and the Internet. The DMA requires all members to adhere to a Code of Practice based on international norms. This is the main self-regulatory body in South Africa for maintaining good and ethical marketing practices that respect consumers' privacy (The DMA, 2000).

There has been little research done on the size of the South African database marketing industry, but the DMA of South Africa stated that the sector is relatively small if compared with other countries (DMA: Industry most frequently asked questions, 2000).

5.3.2 Code of Practice of the Direct Marketing Association of South Africa

As stated before, the DMA of South Africa recognises the world wide accepted privacy principles, although all the principles have not yet been explicitly entrenched in the South African Bill of Rights (The DMA, 2000).

The following are the DMA's Code of Practice, all of which have been incorporated into the Open Democracy Act of 1998 (The DMA, 2000):

- Personal data should be collected and processed in a fair and lawful manner;
- The purpose of data collection should be explicit and legitimate, and data may not be used for other incompatible purposes;
- Data used by bodies should be accurate and up to date. It should be adequate and relevant for the purpose for which it was collected and is used;
- The information should not be used for any purpose without the data subject's knowledge, and every data subject must be offered the right to opt out of disclosure of information to third parties;

- There should be a right of access to information and a right to object on compelling and legitimate grounds;
- Companies should consider the sensitivity of information. Security measures should be implemented and unauthorised access prevented; and
- Member companies must subscribe to the Media Preference Service.

The DMA's Code of Practice has two main purposes. Firstly, it stipulates criteria for professional conduct for marketing professionals. Secondly, when conflict of interest exists between database marketers' practices and consumers' privacy concerns, the Code's rules form the basis of arbitration (DMA: Code of practice, 2000).

In addition to the principles regarding the protection of privacy in traditional media, the database marketing industry is active in developing online principles in order to avoid governmental regulation. Principles such as online notice and opt out, the sending of unsolicited e-mail advertising messages and online marketing to children have already been addressed by the industry (DMA: The privacy file, 1998).

South African consumers perceive "consumer choice" and "empowerment" as the most important principles that need to be in place. These enable consumers to make decisions and choices for themselves, hence obtaining more control over the use of personal information. The DMA of South Africa named these two principles the "Mantra of the Direct Marketing Industry" (DMA: The privacy file, 1998). The responsibility of complying with the DMA code of practice and principles rests primarily with the individual database marketers who joined as members of this association (DMA of South Africa: Code of practice, 2000).

All reasonable steps have thus been taken to ensure that South Africa's principles comply with internationally accepted principles so South Africa does not stay behind. The rest of this chapter will mainly focus on internationally accepted data principles that have been applied to different extents in other countries (The DMA, 2000).

5.3.3 Online principles

Several organisations have developed online informational privacy principles, but two sets of principles are generally accepted and adopted. The FTC from the United States of America developed the first set of five principles, namely Notice, Choice, Access, Security and

Enforcement. It serves as guideline for many other organisations when developing information privacy principles. The Organisation for Economic Development (OECD) developed a second important set of eight privacy principles. The FTC's five principles, together with the eight principles accepted by the OECD will form the focus of the discussion on online principles.

5.3.3.1 Notice/awareness principle

The FTC (1996) indicated that notice of information practices is an essential first principle in advancing information privacy, but especially online privacy. This principle is a prerequisite for implementing the other fair information practice principles that will be discussed in this chapter (FTC, 2000). At a minimum, notice should include the identity of the collector of the information, the intended uses of the information, and the means available to consumers to limit the disclosure of personal information to others (FTC, 1996). Notice may also be given regarding the following: third parties that might gain access to personal information; hidden data collection methods employed by the site; whether provision of requested information is necessary or voluntary; and what steps are taken by the data collector to ensure confidentiality and quality of data. It is important that the notice is clear and not ambiguous. Absence of a "notice" restrict a consumer in making an informed choice about whether and to what extent, to disclose personal information (Valentine, 1999). The FTC (2000) indicated that an average of 77% of web sites display the Notice-principle.

5.3.3.2 Choice/consent principle

Choice is the second principle that is widely accepted. According to this principle, database marketers should obtain consumers' consent regarding any use of information beyond that necessary to complete a transaction (FTC, 2000). Therefore, consumers should be able to exercise control on secondary internal and external uses of personal information. For example, internal secondary uses involve placing the consumer on the data collector's mailing list for future marketing purposes, and external secondary uses involves the transfer of data to third parties (FTC, 1998a).

There are three options for database marketers wishing to grant consumer choice or consent: opt-in, opt-out and selective choice. Privacy advocates favour an "opt-in" approach that requires prior consent to any collection or commercial use of personal information. From a

privacy advocate's point of view, individuals have a property interest in personal information and the opt-in approach is the only means for maintaining the privacy of personal information unless an individual discloses such information. Conversely, industry representatives prefer an "opt-out" approach, which allows personal information to be used without prior consent until consumers notify marketers that personal information is not to be used in specified ways (FTC, 1996). The last option, selective choice, permits consumers to give limited consent to certain kinds of data to be collected or used. (Valentine, 1999). The degree of choice provided will vary across different companies. For example, choice can be given for both external and internal secondary information uses, or otherwise only with respect to external secondary information uses according to the FTC (1998a).

5.3.3.3 Consumer access principle

Access is yet another fair information principle, which is important for the protection of consumers' information privacy. According to this principle the data collector should offer consumers, reasonable access to the information collected about them, together with a reasonable opportunity to review information. Database marketers should also allow consumers to correct or delete inaccurate or other specific information. "Reasonable access" refers to the costs and convenience of accessing such information (FTC, 2000). Entities have the responsibility to maintain the collected information's accuracy and must take the necessary steps to protect it from loss or misuse (FTC, 1996).

However, the FTC (1996) suggested that marketers do not generally provide the opportunity for access to personal data. To the contrary, many have notices, which stipulate: "any information you provide becomes the property of the data collector." The FTC (2000) stated that the Commission would grant marketers recognition for giving access for any one of the following disclosures: when allowing consumers to review some personal information; have some inaccuracies in personal information corrected; and have some personal information about consumers deleted. Thus, the FTC do provide for some flexibility between both different database marketers and consumer needs.

5.3.3.4 Data security/integrity principle

Security measures needs to be in place to ensure that data collectors take reasonable steps to ensure that collected information is accurate and secure from unauthorised use according to

the DMA of the United States of America (Austin and Reed, 1999: 5). The OECD also suggested a security safeguard principle that involves procedures to protect against loss, corruption, destruction, or misuse of data (O'Leary, 1994). The FTC (1996) stated that the security of personal information is essential if database marketing activities, were to flourish. It is thus necessary for database marketers to address this issue. Security and integrity of data can be ensured by, for example, the use of reliable sources of data, and the cross-referencing of data to ensure its creditworthiness (Valentine, 1999).

It is, however, difficult to implement security measures because new threats and information technology will continue to evolve and the need for security will change accordingly. Data collectors should attempt to provide "adequate security" for consumers and it is important to note that the security measures will differ according to the nature of data collected. Security practices could also be disclosed to consumers to enhance consumer trust (FTC, 2000).

5.3.3.5 Enforcement principle

It is necessary to use a reliable mechanism to ensure the effective implementation and compliance with fair information practices. Self-regulatory programs could ensure enforcement and redress by incorporating periodical compliance audits, objective investigation of consumer complaints, and a dispute resolution mechanism (Valentine, 1999). An example of such self-regulatory enforcement program is privacy seal programs. A company may disclose a privacy seal on compliance with the accepted principles (FTC, 2000). Government enforcement through legislation might also be an alternative option for determining compliance with data principles according to the FTC (Valentine, 1999).

5.3.3.6 Specific principles regarding children

Children's privacy is in particular a great concern that needs to be addressed. This is especially due to children's vulnerability to database marketing practices. Child advocates and parents demand that parental consent should be obtained, before database marketers collect and use children's information, the reason being that children lack the developmental capacity or moral judgement to determine whether it is appropriate to provide personal information to a third party. Several problems are associated with the implementation of principles related to the collection and use of children's data. First, it is very difficult to determine the age of a child visiting a web site and whether parental consent has been

obtained. Second, there is a difference of opinion regarding the appropriate age that would require parental consent for collection of children's information. Some experts argue that children under the age of sixteen needs parental consent, while others hold that thirteen would be an appropriate age for obtaining parental consent. Third, it has also been suggested that parents are responsible for information flow affecting children and that parents would be best able to have determined the age at which children are capable of independently engaging in online activities and thus be exposed to database marketing activities. Parents could implement parental empowerment tools to regulate and control information collection and dissemination from children (FTC, 1996).

The privacy principles discussed earlier could also be applied to protect children's privacy. However, additional guidelines and principles have been developed by several institutions to protect specifically children from deceptive and harmful online database marketing practices. These will be outlined in the following paragraph.

First, reference will be made to principles that address data collection from children. These principles include:

- Collection limitation – Children have a right to both anonymity and autonomy and therefore, the data collector should be able to justify why data collection is appropriate. For example, marketers' could encourage children to select "screen names" for online activities according to the Center of Media Education (CME) (Austin and Reed, 1999: 593).
- Parental consent – Parental consent is necessary prior to the collection of a child's data under the following circumstances: when the data collector would be able to contact the child either offline or online; and when the information is disseminated to third parties (FTC, 1998a).
- Appropriateness of content and terminology – All information should be written in a language that children could understand, including privacy policies, disclaimers, and general data practices. Links to other Internet sites, which may contain inappropriate content or terminology should be limited according to the Council of Better Business Bureaus' Children's Advertising Review Unit (CARU) (Austin and Reed, 1999: 600).

Second, the CME (Austin and Reed, 1999: 593) proposed the principles that address the use of children's data. These include:

- Use specification/use limitation – Data may only be used for purposes indicated and should not be used for other database marketing purposes.
- Data quality – Data collectors should protect children's data from unauthorised access by third parties.
- Parental Participation – Parents have a right to inquire about information collected from children by data collectors. Also, the FTC (1998a) stated that parental involvement is the key in successful implementation of principles regarding children' personal information.

Lastly, general guidelines regarding database marketing practices were proposed by CARU (Austin and Reed, 1999: 600). These include:

- Avoid incentives in exchange for a child's disclosure of personal information about themselves and relatives;
- Marketers should not create unrealistic expectations in children when promoting products or services;
- Avoid one-to-one marketing because this puts to much pressure on a child; and
- Clearly separate selling or marketing activities from entertainment and learning activities.

Database marketers need to implement these principles in order to avoid governmental intervention. However, industry self-regulation would most probably not provide an adequate level of privacy for this vulnerable group of consumers, but database marketers could try to limit the amount of governmental interference.

5.3.3.7 Principles proposed by the Organisation for Economic Development

The OECD (OECD guidelines, 1980) has adopted the following eight principles of data protection, which is relevant to protect both adult consumers and children's privacy:

- Collection Limitation Principle – data may only be obtained by lawful and fair means, while certain sensitive data should not be collected without the data subject's consent.
- Data Quality Principle – data should be relevant for the indicated purposes, and it should be accurate, complete and up-to-date.
- Purpose Specification Principle – the purposes of data should be identified prior to data collection and if data are not used for these specified purposes it should be destroyed.
- Use Limitation Principle – the data subject's consent or authority by law is necessary before data can be used for other purposes than specified.

- Security Safeguards Principle – procedures must be implemented to secure data loss and misuse of data.
- Openness Principle – information practices should be disclosed to consumers so they have knowledge about possible information collection, storage and use or alternatively, means should be readily available so the data subject can establish the nature of personal data.
- Individual Participation Principle – firstly, the data subject (a consumer) should have a right to know whether or not a data controller (a database marketer) has captured one's data and secondly, the consumer should have access to data in order to correct or erase incorrect data.
- Accountability Principle – a data controller should be responsible for complying with all of these principles.

24 countries, including Australia, Austria, Belgium, Canada, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States have adopted the OECD guidelines. The guidelines have not been incorporated in all the countries' statutory laws and all the countries have not adopted all eight guidelines. Rather, the level of participation varies slightly from country to country (O'Leary, 1995).

5.3.3.8 Other principles

In addition to all the above-mentioned institutions who have developed guidelines and principles regarding the protection of consumers' and especially children's privacy, there are a number of others, which proposed similar principles. The following important institutions of the United States of America have, apart from those already mentioned, all contributed to the formulation of internationally accepted standards on privacy:

- The Electronic Privacy Information Center with its Code of Fair Information Practices (2000);
- The National Information Infrastructure Task Force (NIIFT) (Varney, 1996);
- The DMA (although the DMA's principles did not recognise several crucial principles which have been widely accepted) (Mummert, 1997);
- The International Federation of Direct Marketing Associations based in the United States of America (DMA: Online marketing principles, 2000); and
- The International Chamber of Commerce (ICC) (DMA: Code of practice, 2000).

5.3.4 Industry initiatives

In addition to complying with accepted privacy principles, there are several other industry initiatives that may enhance consumer privacy. The next section will briefly refer to typical industry initiatives.

5.3.4.1 Media Preference Service

The Media Preference Service of the DMA of South Africa (DMA: The privacy file, 1998) includes three areas of consumer preference:

- Mail Preference Service, which allows consumers to opt out of receiving unwanted direct mail;
- Telephone Preference Service, which allows consumers to limit unwanted telemarketing calls; and
- Fax Preference Service that enables consumers to discontinue fax marketing.

Basically, this free service gives consumers the option to be excluded from mail, telephone and fax databases or lists. Consumers need to request the removal of names and other personal information from marketers' databases. A copy of this record or new database is made available to all DMA members on a quarterly basis. Companies have to delete all the information about individuals listed on these database copies, by putting names on an in-house suppression list. This would prevent database marketers from using or disclosing information from individuals that appear on these lists (DMA: The privacy file, 1998).
The Media Preference System is an example of an opt-out approach and its implementation demonstrates the industry's commitment to proactive privacy protection. It also prevents, to a certain extent, privacy advocates from promoting strict privacy legislation (DMA: The privacy file, 1998).

5.3.4.2 Education

Successful self-regulation programs require the promotion of consumer awareness, proactive policing, and communication with legislators. It is necessary to educate both business people and consumers on issues related to database marketing activities and consumer privacy to ensure effective implementation of self-regulation efforts (DMA: The privacy file, 1998). Consumers generally lack knowledge of collection and use of personal information and do not

understand the potential consequences of disclosing information. Consumers therefore need guidance on how to protect personal information. Consumers should also be made aware of possible trade-offs that exist between better product and service offerings, which result from access to more consumer information. In addition, consumers should especially be educated about privacy rights and practices involving children according to the FTC (1998b). Education is an essential tool for promoting consumer privacy because it could empower consumers to make a more informed choice regarding the control of personal information (FTC, 1996).

5.3.4.3 Infomediaries

"Infomediaries" are entities, which operate as information brokers between consumers and other companies. It provides to some extent protection against the invasion of consumer privacy, while securing financial gain for consumers in exchange for the release of personal information. However, individuals are sceptical to rely on a single firm to protect personal privacy unless the firm has a very good reputation in this particular industry. This is mainly due to the readily availability of one's personal information from several other information sources (The end of privacy: The surveillance society, 1999: 23).

5.3.5 Enforcement mechanisms for self-regulation

Enforcement mechanisms need to be in place to ensure effective self-regulation. Reference has previously been made to self-regulatory efforts in the United States of America that seemed to fail because of a lack of effective enforcement mechanisms. Enforcement mechanisms are necessary to monitor the implementation of industry programs, codes of practices and other industry initiatives. The next section will refer to available enforcement mechanisms.

5.3.5.1 Consumer Affairs Committee of South Africa

The Consumer Affairs Committee (formerly called the Business Practices Committee) is a statutory body formed in terms of the South African Harmful Business Practices Act. The committee has jurisdiction over all business practices in SA and reports to the Minister of Trade and Industry. In addition, the committee has far-reaching legal powers (DMA: The consumer affairs committee, 2000).

The Committee approved the DMA's Code of Practice in terms of the Unfair Business Practices Act and therefore, the Code of Practice was approved and authorised by government (DMA: Negative option marketing, 2000).

5.3.5.2 Third party enforcement programs

Third party enforcement programs could enhance the implementation of privacy principles. These programs offer identifiable symbols to companies or database marketers as a signal to consumers, indicating whether database marketers comply with certain predetermined policies. These symbols can be displayed, for example, on competition entry forms. Third-party enforcement programs should have procedures in place to ensure compliance with policies and for resolving consumer complaints (Effective enforcement of self-regulation, 1998).

An example of an online equivalent is Privacy Seal Programs. Seal programs involve awarding of a seal to database marketers' sites that comply with the program's privacy principles. Database marketers on Web sites are monitored through periodic reviews. This will ensure that those displaying the seal continue to comply with the privacy policies and remain consistent with its privacy principles (Effective enforcement of self-regulation, 1998).

5.3.5.3 Evaluating self-regulation as means for regulating consumer privacy

As previously mentioned, the majority of industry organisations like the DMA of South Africa believe the most effective means for addressing consumer privacy concerns are through self-regulation (DMA: The privacy file, 1998). In addition, the FTC (1998a) stated that self-regulation, rather than legislation, is preferred in protecting consumer privacy because of the rapidly evolving nature of information technology that raise consumer privacy concerns. Self-regulation would enable companies to respond quicker than legislation to the fast changing information technologies and consequently also to changing consumer concerns. Another advantage of self-regulation is that when regulation is voluntarily adopted, by implementing principles or codes of conduct, the compliance thereupon tends to be greater than when legislation is being enforced. Industry experts, who understand marketing practices and conditions, could develop voluntary codes of conduct (Valentine, 1999). A further argument for self-regulation acknowledges that disparities could evolve when countries employ national legislation. Disparities can limit the free flow of personal data

across borders and these flows are bound to grow further with the widespread introduction of new information and computer technology. Restrictions on these cross-border flows could disrupt international commerce and particularly database marketing efforts (OECD guidelines, 1980).

Unfortunately, self-regulatory efforts have not been very successful to date because of several implementation problems. The majority of companies fail to comply with the basic privacy protection principles such as notice, according to research done by the FTC (1998b). One has to remember that companies do tend to value profits more than consumer privacy and unless database marketers are forced in some way to adhere to industry principles, there would be no incentive to do so. An effective enforcement mechanism for self-regulation efforts is essential for providing adequate levels of consumer privacy.

Therefore, self-regulation efforts are a useful means for protecting consumer privacy, but successful implementation requires strict enforcement mechanisms. The alternative otherwise seems to be law enforcement.

5.4 LAW ENFORCEMENT

Different perceptions on what constitutes an invasion of privacy exist across countries as well as within cultures. Consequently, different laws and regulations will be implemented across countries to regulate the specific marketing industries' and consumers' privacy needs.

Law enforcement should only be considered if self-regulatory efforts do not ensure an adequate level of consumer privacy. When developing a proposed legislative model it should set out a basic level of privacy protection for consumers. However, legislation should allow industries to choose their own means for ensuring consumer protection. Government's role is to ensure that industry members comply with whatever means they have decided upon. Industries differ and therefore would require different fair information practices. Different industries' information practices could however be based on general statutory guidance (FTC, 1996).

Thus, government intervention as means for regulating consumer privacy through legislation are seen as a last resort because it restrain marketers' innovation and creativity that

accompany database marketing practices. This argument is also supported by the quote that follows below (FTC, 1996).

> "There is nothing like an absence of regulation for stimulating innovation"
>
> (The end of privacy: The surveillance society, 1999).

5.4.1 The role of government in regulating consumer privacy

The FTC stated that government's role in protecting consumer privacy is to bring the industry, consumers and privacy advocates together. This can be done by government initiatives such as workshops where all parties should be educated and informed about the advantages and disadvantages of marketers' need for information and consumers' need for privacy. Government could also encourage and support effective self-regulatory programs, although such a system has not yet emerged. Incentives or penalties could be established to ensure that self-regulation is effective and consumer privacy is being protected (FTC, 1996).

5.4.2 Law enforcement in different countries

Different countries have employed various methods and legislation for addressing consumer privacy concerns and these countries have succeeded in varying degrees in protecting consumer privacy. Although all protection measures are unique in some manner, one has to recognise the necessity of a coherent policy for measuring success (Pincus and Johns, 1997: 1239).

Law enforcement is typically restricted to a specific country or group of countries, such as the European Union. Laws are generally developed based upon accepted principles of privacy protection within the particular country. It is very difficult, if not impossible to configure different laws in different countries. Therefore, legislation cannot be a means for universal and global protection of privacy and it needs to be complemented with other privacy protection means (Raab, 1997: 167–168).

The following sections will briefly refer to legislation related to consumer privacy, which have been adopted in different countries.

5.4.2.1 United States of America

The United States of America is in essence unregulated with respect to the implementation of fair information practices and principles (Petrison and Wang, 1995: 35). Especially when compared to other countries, the United States of America has relatively low privacy protections for both public and private sector data. The First Amendment's guarantee of free speech allows companies and database marketers, freedom to use personal information just as they wish (Privacy Inc' Consumer Privacy Guide, 1998).

The United States of America has mainly addressed the consumer privacy issue by implementing industry self-regulation, although not being very successful in providing adequate levels of consumer privacy. If industry efforts continue to fail to do so, legislation will become the alternative option. In the meantime, however, many have referred to private protection through legislative efforts in the United States of America as a "patchwork approach" because of diverse state and federal approaches (Pincus and Johns, 1997: 1239).

The Privacy Act of the United States of America is limited to legislation that includes only the public sector, while the private sector is covered by isolated and uncoordinated laws, such as the Fair Credit Reporting Act (The protection of privacy, 2000). In 1986, the Electronic Communications Privacy Act (ECPA) was adopted. This legislation regulates electronic surveillance and was intended to establish some balance between consumers' privacy and marketers' information practices. However, Congress stated that privacy would erode gradually, as technology will advance. That was indeed the case and in 1994, the Communications Assistance for Law Enforcement Act (CALEA) was passed in an attempt to ensure that technological trends would not affect or eliminate law enforcement on personal communications (Dempsey, 1997).

5.4.2.2 European Union

The European Union has passed strict legislation to protect consumer privacy and to limit the disclosure of information. This holds problems for trade of which will be discussed briefly. Government agencies regulate marketers' information practices in various ways throughout Europe. The European Union's Draft Directive on Data Protection of 1992 dictates equivalent data protection rules for all countries that wish to continue doing business with any country in the European Community. At some point, the directive threatened trade with the

private sector of the United States of America because of the lack of adequate data protection (Flaherty, 1999).

In 1998, the European Union passed another directive, which stipulates common rules for collecting, storing and transmitting personal data within and between businesses. The same directive offers European citizens a number of rights, such as the right of access to personal data; the right to correct inaccurate data; the right to know where data originated; the right to refuse data use for marketing activities; and the right of access if unlawful processing occurs. This directive again prohibits any transfer of data to a country that does not provide adequate data protection (Valentine, 1999).

The European Union Directive is considered the most advanced legislation for privacy protection and as such may be a valuable model for consideration for countries currently without data protection laws (The protection of privacy, 2000).

5.4.2.3 South Africa

South African database marketing activities have not yet developed to those of the Unites States of America and the European Union. Legislation was therefore not considered only until recently. South Africa has enacted the Promotion of Access to Information Act in 2000. This Act implies that everyone has a right to access any information held by the State, and any information held by another person that is necessary to protect other rights. This is however limited to the extent that is reasonably and justifiable within an open and democratic society (DMA of South Africa: The legal environment, 2000).

The South African Harmful Business Practices Act, recognises the DMA's Code of Practice and therefore this code is binding on all direct and database marketing organisations, whether being members of the DMA of South Africa or not (DMA: The consumer affairs committee, 2000).

In addition to the above, the Department of Communications received the mandate in May 1998, to establish an information technology investment cluster with the main objective to develop coherent legislation on information society-related privacy issues (Groenewald and Lehlokoe, 1999).

The South African government have yet to decide on an appropriate legislative approach to regulate database marketers' data practices and to protect consumers' privacy. Possible models for consideration are discussed in a latter part of this chapter.

5.4.3 Law enforcement and privacy of children

Children are very vulnerable to marketers' information practices because children do not have the same developmental capabilities as adults and cannot distinguish right from wrong. Therefore, children require separate provisions in respect of privacy protection legislation.

The United States of America institutionalised three Acts, which specifically addresses children's privacy on the Internet. These include the Federal Trade Commission Act, the Communications Decency Act, and the Child Online Protection Act (Austin and Reed, 1999: 591). A brief reference to each of these are justifiable on the grounds that South Africa can utilise these acts as starting point when considering legislation regarding the protection of children's privacy.

5.4.3.1 Federal Trade Commission Act

The Federal Trade Commission Act of the United States of America is applicable to all advertising mediums and it prohibits deceptive and unfair advertising practices. It specifically refers to children because database marketing practices easily misleads children and therefore, marketers' should avoid deceivable advertisements and products. Children are more receptive to deceptive advertisements and are more likely to respond. For example, database marketers advertise products and claim that if children fill in a questionnaire, names will be places in a lucky draw to win the product. In the meantime, the database marketer only wanted to get hold of the children' information and no lucky draw will actually take place. Such false advertisements with the aim to get hold of information are prohibited by this act (Austin and Reed, 1999: 591).

The FTC issued a clear warning that companies in the United States of America that do not comply with the Federal Trade Commission Act can expect legal action and restrictions on future practices, since protecting children's privacy online is a high priority (Austin and Reed, 1999: 591).

5.4.3.2 Communications Decency Act

The Communications Decency Act (CDA) of the United States of America states that children should not have access to indecent or offensive speech on the Internet, otherwise it is seen as a violation of the act. However, the Supreme Court ruled in the case Reno v. ACLU that the CDA was unconstitutional because it places restrictions on free speech (Austin and Reed, 1999: 592).

The Court argued that online database marketers do not invade an individual's home and that consumers seldom encounter any offensive content by accident. They further argued that marketing on the Internet, like traditional marketing mediums such as the television and magazine, contain explicit material, but consumers have the warnings regarding the content before accessing these material. However, the chances of being exposed to explicit images are much higher on the electronic marketing medium than in traditional mediums (Craig, 1998: 11).

Government legislation poses the problem of being restricted to the country itself and the Internet is a global medium. Online database marketers try to avoid governmental intervention by developing educational programs that would increase parental awareness of possible screening software that might aid in protecting children against harmful database marketing practices (Craig, 1998: 13).

5.4.3.3 Child Online Protection Act

This act, also adopted by the United States of America, was approved in October 1998 and it requires database marketers that sell or transfer harmful material on the Internet, to restrict its accessibility by children. The aim is to limit children's exposure to indecent material on the Internet, in the same way as restrictions that have been placed on traditional media that contains harmful content (Austin and Reed, 1999: 593).

5.5 MODELS FOR REGULATING CONSUMER PRIVACY

Bennett suggested several models for the protection of consumers' privacy. In addition, Pincus and Johns proposed a model to identify where a country lies on a continuum with no

privacy and complete privacy as anchors. More detailed reference to these models will be made in the rest of this chapter.

5.5.1 Bennett's models

Bennett has proposed five models to categorise data protection systems of different countries. These approaches to data protection can be applied alone, or a combination of more than one approach can be present in a country. When examining these models, it is important to note that they do not offer a qualitative or normative approach. It is also necessary to consider political and social contexts before deciding on the applicable model for a specific country (Pincus and Johns, 1997: 1239).

5.5.1.1 The Voluntary Control Model

The Voluntary Control Model focuses on industry self-regulation, together with little governmental control. This model presumes that the entity, which gathers and uses personal data, has the responsibility to protect such data against misuse, to provide access to data, and to control the disclosure of such data by taking the necessary steps. In order to accomplish the above, it's necessary to appoint an independent individual that needs to ensure the entity's compliance with existing law (Pincus and Johns, 1997: 1240).

The viability of this model depends on three assumptions. Firstly, there should be some law in place that provides a degree of protection for individual's privacy, because it is unlikely that the entity would develop protective measures. Secondly, the appointed individual should be independent enough or external to the company in order to succeed in protecting consumers' privacy. This is necessary because an individual internal to a company would probably regard privacy protection as inferior to cost savings and marketing efficiency that would be the result of less privacy protection. Such an individual would be too subjective to ensure compliance with the law. Thirdly, enforcement will primarily rest on the public, since no or little external governmental control exists. This presume that the public is well informed about data practices such as gathering, use and storing thereof and that the public will take action to claim privacy rights granted by law (Pincus and Johns, 1997: 1240).

The Voluntary Control Model has one major weakness. Individuals' privacy is threatened if abuses by data gatherers continue because of the absence of legal action. Therefore, if entities

are unable to govern themselves, an invasion of privacy will still exist (Pincus and Johns, 1997: 1240).

5.5.1.2 The Subject Control Model

This model proposes that the data subject, or consumer, is responsible to ensure that privacy is being protected. Data subjects have two options available to them: either access to records and the correction of errors, or the initiation of judicial enforcement of privacy rights (Pincus and Johns, 1997: 1240).

The subject control model is only meaningful for protecting privacy when the data subject: is sufficiently informed of the existence, purpose and content of data records; know how to get access to information; and, is able to correct or delete inaccurate or obsolete information. Therefore, individuals have to assert privacy rights in order for this model to succeed (Pincus and Johns, 1997: 1240).

The weakness of this model is derived from one of its assumptions in order to succeed: if society does not claim privacy rights or initiate law enforcement, consumer privacy would not be protected. If individuals do claim the right to privacy, it is because privacy has probably already been infringed. Therefore, this is a relatively reactive protection model (Pincus and Johns, 1997: 1240).

5.5.1.3 The Licensing Model

Unlike the previous two models, this model involves some governmental institution with regulatory and advisory powers to control the data collector and to assist the often relatively unskilled data subject. Thus, the governmental institution is a mediator between data collector and data subject (Pincus and Johns, 1997: 1241).

The governmental institution that aid in the protection of privacy is usually an agency devoted to licensing the establishment of personal information data banks. The agency identifies specific conditions under which data may be gathered, stored, processed and disseminated. Any other relevant aspects of the data system, including changing in procedures are subjected to approval by the agency (Pincus and Johns, 1997: 1241).

The Licensing Model places a higher value on individual privacy in comparison with the models discussed earlier and it allows licences to be created according to the unique needs of each data collector. Conversely, it also has the disadvantage of being too bureaucratic and this might lead to problems for data collectors (Pincus and Johns, 1997: 1241).

5.5.1.4 The Registration Model

This model is similar to the Licensing Model except that it does not involve an agency with regulatory powers. Rather, it acts like a notice system. Registration by data collectors implies adherence with non-binding principles of fair information practices that were developed by the agency. The agency, however, have no authoritative power to enforce compliance with these principles. Registered data collectors have to give notice to the public regarding data practices employed, such as data collection, use and dissemination (Pincus and Johns, 1997: 1241).

The only problem with this model seems to be that any data collection and processing prior to registration is unlawful. This is a popular model and has been implemented by a number of countries (Pincus and Johns, 1997: 1241).

5.5.1.5 The Data Commissioner Model

The Data Commissioner Model comprises of a commission with the power to investigate complaints, constrain the development of databases, review data gathering practices and advise on improvements in data collectors' systems. The commission should also monitor technological advancements that could enhance consumer privacy. However, the commission is without power to prescribe regulations. Therefore, the success of this model depends on the commission's ability to develop good relationships with data gatherers and to educate the public to pressurise those who do not comply with fair information practices (Pincus and Johns, 1997: 1241).

5.5.1.6 Evaluation of Bennett's models

Bennett's models mainly refer to a country's policy choices with respect to which party should have the responsibility for protecting the privacy interests of individuals. The data collector is responsible in the Voluntary Control Model, the data subject is responsible in the

Subject Control Model, and the Government is responsible in the Data Commissioner Model. Responsibility can also be assigned to a combination of actors, for example the data collector and government is both responsible in the Licensing Model and the data subject and government is both responsible in the Registration Model (Pincus and Johns, 1997: 1242).

The value of Bennett's five models is twofold. First, it provides a clear-cut identification of the dominant actors and the most useful combinations thereof, together with a range of possible policy choices available to countries. Second, Bennett's models should be evaluated after the efficiency of a large number of other privacy protection schemes have been measured. This would indicate which actor is the most effective in protecting the privacy of consumers within a given set of environmental factors. One should remember that the importance of the primarily responsible actor would vary between countries. Also, the reliance on the primary responsible actor is just relatively, as the other actors are also important in protecting privacy, although to a lesser extent (Pincus and Johns, 1997: 1242).

5.5.2 Pincus and Johns' Privacy Protection Model

The Privacy Protection Model (PPM) measures the degree of protection offered by a country's privacy protection scheme. Rather than identifying the actors responsible for privacy protection, it evaluates the degree to which individuals are actually protected (Pincus and Johns, 1997: 1242).

The model is composed of two parts:

- A privacy protection index, which is a compilation of the minimum amount of factors that should be evaluated when determining whether a country offers adequate protection for consumer privacy.
- A privacy protection scale, which categorises a country and place a country on a continuum ranging from minimal protection, moderate protection to strong protection. It is assumed that there is not such a thing as no protection or complete protection, but is serves as ideals or anchors on either ends of the scale (Pincus and Johns, 1997: 1243).

Data variables, which refer to factors concerning the collection or use of data, offer certain levels of privacy protection. Data variables are used to complete the protection index and may include the following (Pincus and Johns, 1997: 1244):

- what and how the data is collected;
- the purpose for which the data is collected;
- who is collecting the data and to whom is it being transferred;
- the medium of storage of the data as well as the duration of data maintenance;
- the location of data storage; and
- the timing of notice of data gathering, use or dissemination.

It is important to note that the PPM only measures legal forces for privacy protection and not societal forces, because the latter would not be comparable across countries (Pincus and Johns, 1997: 1244).

5.5.2.1 Structure of the index

Pincus and Johns (1997: 1245) suggested that when evaluating a country's protection scheme, one should consider three areas that have a number of sub-areas for possible protection:

- Notice of data collection and use,
- Restrictions on data collection and use, and
- Remedies available for violations of restrictions on data collection and use.

Each protection area is evaluated according to the relevant protection possibility for that area. With regard to each of these protection possibilities, there are a number of data variables and each data variable is assigned a score based on the extent to which it ensures protection or allow privacy infringement. The index score for each country is compiled by totalling the scores for each protection possibility and the country could then be placed on the PPM continuum (Pincus and Johns, 1997: 1245).

The protection possibilities that exist for each protection area as well as the nature of these will be briefly discussed in the following section. The first index area, namely notice of data collection and used, can be divided into two protection possibilities, namely constructive notice and actual notice. Each of these possibilities can be subdivided into notice to government and notice to data subjects (consumers). The second index area, namely restrictions on data collection and use, has two protection possibilities: restrictions related to government and restrictions relating to private parties. Government has four options by which data collection and dissemination can be regulated: a commission, an investigatory

body, non-binding guidelines and enforcement provisions to give affect to the mentioned guidelines. The third index area, namely remedies, has three possible protection means: potential defendants, regulatory remedies and judicial remedies. When evaluating data variables, one should assess the availability of certain remedies and parties, such as government or industry self-regulatory bodies, to the protection restrictions (Pincus and Johns, 1997: 1245). For example, potential defendants can be evaluated by data variables such as: does the regulations or statutes in question apply to and regulate governmental entities that collect personal data; private parties that use secondary data; and private parties that collect personal data (Pincus and Johns, 1997: 1245-1246).

The "regulatory remedies" and "statutory remedies" protection possibilities are evaluated by data variables such as types of remedies provided under the relevant regulation or statute, for example, restraining orders, punitive damages and the right to inspect and to correct (Pincus and Johns, 1997: 1246).

5.5.2.2 Application of the Privacy Protection Model

The PPM offers a qualitative base from which one can determine what level of privacy protection is offered within a given country and how countries' privacy protection schemes compare with each other. Bennett's models indicated what privacy protection systems could be implemented. The PPM, on the other hand, indicates where countries are located along a continuum of no protection to complete protection as anchors (Pincus and Johns, 1997: 1248).

5.5.2.3 Applying Bennett's models to the European Union and the United States of America

Reference has previously been made to differences in countries' legislation efforts to protect consumer privacy. Pincus and Johns stated that when there are differences between countries' data protection schemes, such as the European Union and the United States of America, unauthorised transmission of data is the sender's liability. Therefore, the sender must be satisfied that the receiving end's jurisdiction provides adequate protection for privacy. For example, if the European Union (with its stricter protection system), transfer data to the United States of America (with its relatively unregulated system), the European Union has the responsibility to determine whether the United States of America provides adequate

protection. If a dispute exists, a dispute resolution in an international forum will be required (Pincus and Johns, 1997: 1248).

The United States of America is primarily regulated by the Voluntary Control Model but also contains elements of the Subject Control Model. Further, tort law is regulating the private sectors of the United States of America (Pincus and Johns, 1997: 1245). However, the Voluntary Control Model failed in regulating database marketing activities and to ensure proper consumer privacy in the United States of America (Pincus and Johns, 1997: 1248). For any system to be successful in the United States of America, protection must originate from the entity with the greatest interest in protection. This entity needs to ensure and monitor the privacy protection scheme. Unfortunately, individuals are sometimes unaware of the invasion of the right to privacy and in such a situation outside monitoring would be called for (Pincus and Johns, 1997: 1251). The European Union, on the other hand, has elements of both the Registration Model and the Data Commissioner Model (Pincus and Johns, 1997: 1248).

5.5.2.4 Limitations of the Privacy Protection Model

If the PPM is to be considered for implementation, more research is necessary in respect of the weights that should be assigned to the different data variables referred to in this chapter. In the Pincus and Johns' study, the weighs were determined subjectively. Pincus and John suggests that research should consist of a survey of perceptions on privacy protection as well as on privacy invasion based on the existence or non-existence of a data variable. These perceptions might be different across countries and therefore the index should be culturally corrected to accommodate different perceptions.

The PPM does not solve the problem comparing different cultural and legally accepted definitions of privacy, but it effectively indicates a general and comparative view on different countries' privacy protection schemes. Therefore, the PPM does not suggest specific cultural or legal views on privacy for each country, but rather, gives an indication of differences in the level of privacy protection offered within different countries. Further development of the PPM is necessary to make it applicable on a sector-by-sector basis. This would make it possible to compare the level of privacy protection offered by different industry sectors. For example, one can establish what levels of consumer privacy are necessary within different

product and service industries and compare if the industry under consideration adhere to these requirements (Pincus and Johns, 1997: 1250).

The use of the PPM does not presume that the highest regulation and range points on the scale are the most appropriate for every country. Of course, different points on the scale would be applicable to different countries. The end points "no protection" and "complete protection" would not be the best solutions because over-regulated or under-regulated areas are just unworkable as the opposite (Pincus and Johns, 1997: 1250).

5.6 SUMMARY AND IMPLICATIONS FOR DATABASE MARKETING

Advancements in database technology raised several social and ethical considerations regarding its commercial use. It can be foreseen that database technology will continue to improve and at each stage of improvement new social, ethical and privacy issues will warrant consideration. Although there is no easy solution to the invasion of privacy, compromises and co-operation between the groups affected could bring some balance in the diverse interests.

There are several approaches to the protection of consumer privacy: The use of information technology, self-regulation and government intervention. These approaches as well as a possible privacy protection model will be evaluated in Chapter 6. Only a brief summary on the approaches will follow. Privacy-enhancing information technology is an effective tool for protecting consumer privacy. It is flexible enough to change quickly to shifts in marketers' data practices and the consequent shifts in consumer privacy concerns. It provides for anonymous browsing of the Internet and offers more consumer control over the collection and dissemination of personal information. Privacy-enhancing information technology as a tool for the protection of privacy could be used in addition to other tools that have been discussed.

Self-regulation is another means for promoting consumer privacy. Industry efforts include the development of principles to which companies must adhere to, and the implementation of several industry initiatives, such as a Media Preference Service. Industry efforts also include educational programs to enhance consumer and business awareness regarding data practices, consumer concerns and the possible trade-offs that needs to be considered. The efficiency of self-regulation is limited due to the lack of an effective enforcement mechanism. In South

Africa, the DMA is the main regulatory industry body, but they do not hold much authoritative power.

Law enforcement with the purpose of protecting consumer privacy is considered to be the last resort. Government intervention through the adoption of legislation poses restrictions on marketers' innovation and creativity. Legislation would most likely ignore the benefits and trade-offs provided by marketers' data practices. Government should rather assist in promoting consumer awareness through educational programs and could act as mediator between consumers and the database marketing industry. It has been proposed that legislation related to children's privacy issues should be adopted because children are such a vulnerable consumer group. If other protection remedies seems to fail, government intervention will become the alternative.

Bennett proposed several models for the protection of privacy. These include the Voluntary Control Model, the Subject Control Model, the Licensing Model, the Registration Model and finally the Data Commissioner Model. These models indicate which parties should be held responsible for monitoring and initiating the protection of privacy. Pincus and Johns proposed another model, namely the Privacy Protection Model. The value of this model lies in its qualitative nature, which measures a country's level of privacy protection in relation to other countries by plotting a country on a continuum with endpoints, no privacy and complete privacy. Bennett's models and Pincus and Johns's model could be useful in evaluating an appropriate system for protecting consumer privacy and also for evaluating the effectiveness of such a system.

When designing a policy for the protection of privacy one needs to consider all the available means and the different combinations thereof. The successful implementation of a protection policy in one country does not suggest that the same policy would be effective in another country because marketing practices and consumer concerns in different countries vary to a great extend. Therefore, it is necessary to consider each and every factor that may have an influence on the development of an appropriate policy.

A combination of the Registration Model and the Data Commissioner Model has been proposed as possible model for regulating consumer privacy in South Africa. Chapter 6 contains an evaluation of these models.

CHAPTER 6

CONCLUSIONS AND A SUGGESTED MODEL FOR REGULATING DATABASE MARKETING PRACTICES IN SOUTH AFRICA

This chapter refers to the conclusions drawn from previous chapters as well as possible models for protecting consumer privacy. More specifically, reference will be made to a model suggested for South Africa, considering the conditions and challenges unique to the South African environment.

6.1 THE CONCEPT OF PRIVACY

Chapter 2 referred to three meanings attached to the concept of privacy. First, reference was made to the general meaning of privacy that acknowledges that all human beings desire some degree of territorial privacy. Secondly, the legal interpretation of privacy suggests that privacy is a human right worth protecting, although not always explicitly adopted in legislation. Legal definitions of privacy acknowledge privacy of the person (physical privacy) as well as privacy of a person's information and communication (information privacy). Thirdly, reference was made to the concept of consumer privacy. Consumer privacy focuses primarily on privacy of a consumer's personal information. Further conclusions are mainly based on the interpretation of privacy within the consumer-marketer context.

6.1.1 General meaning of privacy

Different aspects of a person's privacy were addressed in Chapter 2. Literature suggests that all human beings, whether human or animal, have a need for personal privacy. One can however, only expect a reasonable amount of privacy when participating in society. The more one interact with other members of society, the more one could expect to compromise a certain amount of one's privacy. This implies that when consumers participate in a business transaction, consumers could expect that a degree of personal privacy will be invaded. The seller of a product or service will require some information to complete the transaction. If, however, the information is then used for purposes other than necessary to complete the transaction (and it was not agreed so by the consumer), it could be regarded as an invasion of privacy. The reasonable-man principle becomes inevitable in determining when consumer privacy is being invaded. This reasonable-man principle led to problems for marketers

because what is reasonable for one is not necessarily reasonable for another. This is especially a problem for database marketers that work within different cultural contexts or that market products and services globally. The meaning attached to privacy will differ across cultures and therefore what a culture perceives as fair and reasonable information practices will vary. Marketing practices employed in a certain country might be seen as offensive or invasive in another. The problem is, however, that it is very difficult to define "fair information practice". One should therefore identify which data practices are acceptable within a given society. Cultural differences were evident in the British-American example. Americans are much more receptive to database marketing practices than the Britons. Cultural differences are prominent amongst both consumers and database marketers and this could also lead to different database marketers' views on acceptable marketing practices. Members within the database marketing industry with different views on database marketing practices could experience difficulty with industry codes of conduct.

6.1.2 Legal meaning of privacy

The legal definition of privacy, hold implications for the regulation of database marketing information gathering and use activities. Currently, few laws and legislation are in place to regulate such activities. Statutory law, common law and specifically the South African Bill of Rights recognises the general right to privacy. The Bill of Rights propose that individuals should have access to information held about them; should be able to correct incorrect information; and should have some protection against the abuse of such information. This implies that database marketers cannot use and abuse consumer information, but should keep the rights of consumers in mind when collecting or using consumer information. Marketers could study the particular legislation, common law or certain accepted practices before entering a market. This will enable marketers to determine compliance with the area's norms. Marketers could then employ legitimate data practices to alleviate consumer privacy concerns.

Generally, the legislature acknowledges privacy as the right to be left alone; the right to the development of the individual personality; and the right to informational privacy. Legislation should however be viewed within a social context. Consumers cannot expect to be left alone because consumers participate in society's exchanges of goods, services and information. The right to the development of an individual personality is at stake when database marketing practices involve the collection and use of information from vulnerable parties such as

children. These data may be disseminated to third parties whom may have harmful intentions and as such children could be exposed to, for example, inappropriate or explicit material. Legislation also acknowledges information privacy, which may be invaded when marketers obtain personal data in an intrusive way. Privacy legislation holds implications for marketers. If marketers do not comply with the right granted by constitution, the consequence could be legal action.

Database marketers need to develop codes of conduct that reflect legislative definitions of privacy. The lack of coherent and specific data protection or consumer privacy protection laws in South Africa, however, resulted in lack of marketers' concern for privacy issues. Legal interpretations of the concept of privacy will vary across different cultures and countries. The implication for database marketing is that different industry codes of conduct will apply within different cultural settings. Database marketers should therefore adapt according to the general sense of privacy within a specific country.

The constitutional right to privacy acknowledges that a person could expect a reasonable amount of privacy when participating within a society. One should therefore expect that within a context where an exchange relationship exists, between database marketers and consumers, some privacy would be lost. The more a consumer interacts with businesses and the more transactions the consumer engage in, the more privacy will be lost. There exist a trade-off between one's need to interact socially and one's need to maintain privacy.

The privacy construct, as one knows it today, has been developed since the 1890's. As mentioned earlier, various definitions of privacy have been formulated, but there is still no universally agreed-upon meaning of privacy. Reference was made to several definitions of privacy, but authors stressed mainly two points – informational privacy and physical privacy. These core dimensions of the privacy construct were extended by Prosser's legal torts, which are widely accepted by courts and legal entities. However, only two of the torts, namely disclosure and appropriation appears to be relevant within the database marketing context. The direct legal implication of disclosure for marketing practices is that highly confidential information, such as medical, financial and sexual information should be treated as such. Database marketers should be sensitive to consumers' concerns when sensitive types of information are involved. The direct legal implication for appropriation is that only the collection and use of individual-level information will be seen as an invasion of privacy and should be limited, especially where consumers have not granted explicit or implied consent to

such data collection and use practices. Database marketers could however use group-level information without invading a consumer's privacy.

6.1.3 Consumer privacy

A further perspective on privacy relates to privacy from a consumer's point of view. Consumer privacy predominantly focuses on informational privacy, but in addition it also recognise physical privacy. Social interaction and the social environment, in which consumers participate, create the need for privacy. Consumers' need for privacy is therefore, in conflict with the need for social interaction and the need to participate in commercial exchange relationships. Consumers should weigh the social and economic benefits received in exchanging personal information, and accordingly decide what level of privacy is desirable. Complete privacy is not the ultimate objective, but rather consumers desire a reasonable level of privacy as expected by society.

6.2 MARKETER PERSPECTIVES ON DATABASE MARKETING PRACTICES

The next part of this study focused on the influence of the information age on marketing activities. Information technology, especially computer information technology made society much more transparent. Advancements in information technology and the development and expansion of the Internet hold implications for marketing activities. It resulted in a shift from traditional marketing practices to concentrate on database marketing practices that involve the collection, processing and dissemination of vast amounts of consumer information. Marketers claim that the utilisation of detailed consumer information is of utmost importance for effective marketing programs. Consumer information could now be obtained easier, cheaper and faster due to the availability of information technology. Most experts agree that personal information will increasingly become available to those marketers who wish to use it. Consumers also benefit from new information technologies. Database marketers are able to offer improved products and services, which is more customised than before. To the contrary, consumers also believe that personal privacy is being threatened by this readily available consumer data. Consumers are concerned about how personal information is being used by marketers.

Several methods for obtaining consumer information were discussed in Chapter 3. These include information obtained as part of the marketing exchange process, through public

databases or through electronic means. The majority of information is collected through daily transactions, public databases and through electronic means, such as clickstream, cookies, software, and e-mail. More specifically, the marketing exchange process involves information obtained from sources that include interactive television and videotext, telephone's automatic number identification system, 0800 and 0900 numbers, and automatic diallers; CD-ROM's and secondary sources of information. Similar methods are used for collecting children' information and this raises consumer privacy concerns.

Marketers have several uses for consumer information. Data from various sources are aggregated and then used to compile consumer data lists and databases. Data mining techniques are used to analyse such data and for identifying consumer wants and needs. The information enables marketers to segment consumer markets and to develop targeted advertising messages and customised products and services. To conclude, such information improves the overall marketing strategy and results in more efficient marketing practice. The availability of consumer information are therefore of great importance to database marketing. Marketers will continuously attempt to obtain such data and use it in a meaningful way. Inappropriate use for consumer information however, raises consumer privacy concern. This may include the use of children' data, secondary use of consumer data and the use of consumer data for financial gain. These, and the other issues discussed, need to be addressed and solutions need to be found to ensure sustainable database marketing practices in future.

6.3 CONSUMER CONCERNS FOR PRIVACY

Database marketing activities, which involve the collection and use of consumer information, raise several consumer privacy concerns. One can distinguish between several consumer clusters according to consumers' attitudes regarding privacy. The typical South African consumer could be classified as a "pragmatist". Pragmatists are concerned with privacy to the extent that consumers are exposed to database marketing activities. The South African database marketing industry is still in its infancy and as the industry progresses, and consumers become more knowledgeable, privacy concerns will probably also increase.

The primary drivers of consumer concern are the general lack of knowledge on data collection and use, the type of information collected and the amount of control consumers have over subsequent use of data. Other factors that raise consumer concerns include: the use of personal information to identify specific individuals; collection and use of sensitive

information, such as medical and financial data, rather than the collection of demographic and lifestyle data; the volume of information collected and used; secondary information use; the use and dissemination of inaccurate databases; the collection and use of children's data and the lack of benefits received in exchange for information provided. Consumers are also especially concerned about online database marketing practices because of the secrecy in data collection and use. However, concerns may vary depending on consumers' cultural orientation, age, perception on what constitutes good marketing ethics or the specific methods employed to obtain consumer data.

Data practices may evoke consumer privacy concerns, but it is important to note that database marketing activities may hold many benefits for consumers. Improved products and services, and a greater variety of products and services available to the consumer are likely to result from better market research. Consumer information solely used for marketing purposes and to enhance the marketing exchange process is therefore generally not seen as a major concern by consumers. Consumers need to be made aware of all the benefits to make an informed choice on whether to provide information or not, and on whether privacy is really being threatened by database marketing practices. Consumers are generally not concerned with the collection and use of personal information when have given explicit consent or when providing information voluntarily.

6.4 TRADE-OFFS BETWEEN CONSUMER PRIVACY NEEDS AND MARKETER INFORMATION NEEDS

Marketers' information needs and consumers' privacy needs should somehow be balanced in order to prevent strict government intervention. Absolute privacy is not the important social goal but consumers expect a reasonable level of privacy. Awareness of trade-offs between marketers' and consumers' needs should be established through business and consumer education. Compromises from both sides are necessary to reach a more balanced relationship between the two parties.

As a starting point, marketers need to acknowledge that the concern for consumer privacy is a very important issue that needs to be addressed to ensure successful marketing campaigns in future. Database marketers should educate consumers on data collection and use practices and the tangible and intangible benefits received for providing marketers with personal information. Consumers have shown a willingness to give up some level of privacy if they

receive some benefit in exchange. Marketers should also establish a general awareness of possible options consumers may have to alleviate privacy concerns.

Lack of consumer knowledge of database marketing activities, was identified as one of the major consumer privacy concerns. Disclosure of data collection and use practices could therefore alleviate such concerns. Consumers would be more informed about data practices and therefore would have better knowledge on how to protect themselves. The ability to protect oneself, by for example having knowledge of an opt-out system and using such an opportunity, will enable a consumer to enhance personal privacy. More control over personal information will in turn, alleviate consumer privacy concerns.

Marketers could alleviate consumer privacy concerns by considering the small aspects of database marketing that causes concern. Marketers could avoid collecting and storing irrelevant consumer information. It would lead to cost efficiencies if only relevant information is collected and used. This could also alleviate consumer privacy concerns. In addition, marketers could try to use information within a group-level context because consumers are very concerned about the use of information within an individual-level context.

An issue that probably would not be resolved is that of ownership of data. Consumers claim they are the owners of personal data. To the contrary, marketers claim they hold ownership of obtained data because they bear the costs associated with data collection, processing and storage. Hence, database marketers could use the data for any purpose, including selling or renting such data.

The issue of secondary information sources also needs to be addressed. The selling and renting of consumer data for financial gain, especially when inaccurate databases are sold, should be reconsidered. Marketers may gain by using accurate databases, rather than databases compiled not for its accuracy, but rather for its financial benefit. Legitimate sources of data will benefit both the marketer and the consumer. The marketer will be able to target consumers more effectively by using available resources more efficiently. Consumers would receive less mistargeted advertising messages.

Generally, consumers are very annoyed with inappropriate database marketing offers where inaccurate information for example, may lead to misclassifications. Misclassification may be the result of marketers analysing techniques, misinterpretation of data and incorrect

correlations and predictions between suppose to be related factors. Consumers are then targeted with irrelevant products and services. Situations like these could be avoided according to marketers by collecting more detailed consumer information. It should however be avoided by collecting only information relevant to the product and service offer.

Different consumer clusters and consumer types will have different implications for database marketers. Database marketers should determine the target market and whether consumers of this target market are fairly or deeply concerned about personal privacy. Database marketers need to adapt data practices according to consumer differences, whether being cultural, personal or other differences. In general, the South African consumer is currently relatively unconcerned about consumer privacy because of several reasons. Database marketing practices are not as common in South Africa as in other more developed countries. Little experience with marketers' data collection and use practices and therefore, lack of knowledge of such practices, also influence South African consumers' perspectives. As the database marketing industry progresses, marketers will have to address new privacy issues to avoid strict industry regulation or maybe government intervention eventually. Database marketers should especially be cautious in a country such as South Africa with its current focus on human rights. South African consumers would most likely claim privacy rights once having knowledge of data practices which threaten personal privacy.

Consumers appreciate database marketers' need for information and acknowledge some benefits consumers might receive. Consumers are however concerned about certain practices used to obtain information and some specific uses of information are also perceived to be invasive. The constitutional right to privacy acknowledges that consumers could expect a reasonable amount of privacy, but the more consumers participate in the social environment or business exchange relationships, the more could consumers expect that some privacy would be lost. Marketers should thus address the privacy issue by focussing on unreasonable data practices as perceived by society as a whole.

Marketers do need consumer information for more effective marketing programs, but marketers should acknowledge that consumers have certain privacy rights. Consumers' privacy concerns have implications for the regulation of database marketing activities. Database marketers prefer industry self-regulation as means for ensuring consumer privacy and should therefore adhere to industry codes of practice to ensure more effective self-regulation. If self-regulation efforts became insufficient in ensuring adequate levels of

consumer privacy, and if consumers claim privacy rights, legislation would most likely be imposed. Government intervention will restrict database marketing activities, which are essential for the development of effective marketing programs. Marketers should therefore not ignore the raising privacy concerns of consumers but should rather, address these issues to ensure a more balanced marketplace. In reality, all parties should acknowledge that database marketers will not stop collecting and using personal information but will continue to attempt to get hold of consumer data. Regulators should therefore focus on alleviating privacy concerns and limit unnecessary or harmful data practices.

6.5 EVALUATING APPROACHES FOR REGULATING CONSUMER PRIVACY

Advancements in database technology raised several social and ethical considerations regarding its commercial use. It can be foreseen that database technology will continue to improve and at each stage of improvement new social, ethical and privacy issues might warrant consideration. Although there is no easy solution to the invasion of privacy, compromises and cooperation between the groups affected could bring some balance in the diverse interests.

There are three main approaches for regulating consumer privacy: information technology, industry self-regulation and government intervention. These approaches will be evaluated in the following sections.

6.5.1 The application of current information technology as means for regulating consumer privacy

Privacy-enhancing information technology could play an important role in addressing consumers' privacy concerns, which was partly caused by information technology itself. Information technology enables new database marketing practices, which in turn, are responsible for many consumer concerns. Most data collection, storing, interpretation and dissemination are accomplished by electronic means. Rather than focussing on information technology that "invades" consumer privacy, the focus could be on information technology that "enhances" consumer privacy and consequently alleviate consumer concern.

Information technology as means for protecting consumer privacy holds the following advantages. Firstly, information technology applied by database marketers, and which raise

consumer privacy concern, changes frequently. Legislation and industry regulation efforts attempting to protect consumer privacy, are not able to adapt quickly to these changes. Privacy-enhancing information technology that alleviates consumer concerns may change just as fast as the information technology that raises such consumer concerns and could therefore be an appropriate and flexible tool for regulating these technologies. Information technology could especially be used in protecting children's privacy. Information technology empowers parents to obtain more control over the collection and use of data on children, as well as children' exposure to offensive marketing offers. These problems could be addressed by filtering software, which parents install in the computer. Parents have the responsibility to protect children's online activities and should employ information technology to help them in this regard. Information technology therefore provides for anonymous browsing of the Internet and offers more consumer control over the collection and dissemination of personal information.

The application of information technology for addressing consumer privacy concerns, pose the following problems. Firstly, individuals may lack knowledge of available technology that could be employed to obtain more control over collection and use of personal information. Widespread consumer education programs could resolve this problem. Secondly, strong industry-wide and consumer commitment are necessary to ensure the adoption and use of privacy-enhancing information technology. Thirdly, information technology mainly provides for regulation of online database marketing activities and would not be a sufficient tool in protecting more traditional database marketing mediums, such as the television, telephone and unsolicited mail offerings. Lastly, there are currently no effective enforcement mechanisms in place to ensure control over the implementation and use of information technology. The implementation of information technology to alleviate consumer privacy concerns, are therefore likely to be voluntarily by nature.

To conclude, there exist many information technologies that could be employed to alleviate consumer privacy concerns. Information technology is a good supplement to industry self-regulation and government efforts in protecting privacy and could be promoted by enhancing consumer and business awareness on the available information technologies. Industry self-regulation and governmental interference could be used as main approaches for protecting consumer privacy, while privacy-enhancing information technology could be employed to adapt quickly to fast changing information technology that raises consumer concern. Hopefully, future information technological developments will have the capacity to provide

an underlying framework for privacy, providing greater anonymity, confidentiality, and a platform for fair information practices. Information technologies should be a central part of a privacy protection framework because it could provide protection across the global and decentralised marketing mediums where legal or self-regulation may fail.

6.5.2 Industry self-regulation as means for regulating consumer privacy

Industry self-regulation is another approach for regulating database marketing practices. Self-regulation requires all industry members to monitor data practices in order to ensure some degree of consumer privacy. Codes of conduct and industry principles have been developed as guidelines for industry members. Industry regulatory bodies need to ensure that industry members comply with these codes and principles. A private sector response to consumer concerns could also incorporate other industry initiatives such as educational programs to enhance consumer and business awareness on data practices, consumer concerns, and the possible trade-offs that needs to be considered. The industry should also provide for enforcement mechanisms in order to ensure adequate consumer privacy protection.

The main database marketing industry regulatory body in South Africa is the DMA. The DMA of South Africa developed a code of practice similar to international standards and all members have to adhere to this code. In addition, the DMA of South Africa established other regulatory services such as the Media Preference Service that provides opting out of consumer lists. Consumer complaints can be filed at the DMA of South Africa who will investigate the problem and if a wrongful practice has been detected it will be referred to the Consumer Affairs Committee of South Africa.

The question has been asked whether industry should implement an opt-out or an opt-in approach. Should society permit database marketers to use personal information unless and until the individual "opts-out" or should society require database marketers to obtain an individual's consent prior to gathering of personal information? Currently, the South African database marketing industry follows an opt-out process. Those individuals that are concerned about databases containing personal information, could opt-out, and those who do not mind personal information being used, could leave such information on these lists. There are many individuals in South Africa that lack knowledge of marketers' information practices and therefore privacy concern in South Africa is not such a big issue when comparing with other

developed countries. This is due to database marketing practices in South Africa that have not yet progressed to the same level as many other countries.

6.5.2.1 Principles underlying self-regulation

The database marketing industry of the United States of America has incorporated the FTC's principles to regulate data practices and to protect consumer privacy. The FTC proposed 5 main principles, which have been implemented in a number of countries. These principles could also be used in the South African database marketing industry to maintain fair information practices. These principles include notice, choice, access, data security/integrity and enforcement. Marketers should, according to the notice principle, disclose the database marketer's identity, the intended uses of information and the means by which consumers could limit the disclosure of personal information. Although this is the fundamental principle, research suggests that industry members have difficulty to comply with this principle. The choice/consent principle suggests that marketers need consumers' consent before using any personal data, other than being necessary for the transaction. Consumers should also be allowed access to personal information and have some control over subsequent uses of such information. This principle is widely employed in South Africa as part of an industry initiative, called the Media Preference Service that allow consumers to opt-out of marketers' databases. The third principle, access, allows consumers to access data records and correct any inaccurate information. Some marketers argue that collected information is marketers' property and in fact, display notices such as "any information you provide becomes the property of the data collector", which indicate that no consumer access will be granted. Therefore, this principle also has not been implemented efficiently. The forth principle of data security and integrity, suggests that data collectors are responsible for maintaining accurate information and must secure data from unauthorised use. This is an important principle in establishing a trust relationship with the consumer, which is essential for sustainable database marketing campaigns. The last principle, enforcement, necessitates a reliable enforcement mechanism to determine whether data collectors adhere to established privacy principles. The lack of complying with this principle is the main reason why self-regulatory efforts have not been successful yet. The utilisation of an effective enforcement mechanism could enhance consumer privacy.

The above-mentioned principles could also be made applicable to children's privacy, although these principles require parental participation. Children are a vulnerable group and database

marketing practices make it difficult for companies to ensure protection for children. Additional principles, related to appropriateness of content and terminology and to ensure anonymity when exposed to online database marketing activities, have been developed. It still appears as if children's privacy cannot be protected sufficiently by implementing privacy principles and it therefore seems that additional legislation as an enforcement mechanism, will be necessary to ensure privacy of children's data.

The OECD adopted another set of eight principles for data protection. The OECD principles are in essence similar to the FTC's principles, but in addition it restricts collection of certain types of data; data can only be used for specified purposes; and the data controller should be responsible for complying with all of the principles.

There are several essential components of a model or privacy code in order to address privacy concerns. One needs commitment to implementing fair information practices. In essence, this means collecting only timely, relevant, accurate data, keeping it up to date, using it only for purposes announced at the time of collection, disclosing it only in accordance with stated, accepted rules, and granting consumers a right of access to personal information. Database marketers need to reach consensus on how to implement fair information practices because if database marketers disagree, compliance with these principles would unlikely be the result. There should be some responsible entity to promote compliance with the privacy principles and there should be penalties for not complying with such principles.

6.5.2.2 Typical problems associated with industry self-regulation

Industry principles and codes of conduct seem to provide a guideline for stipulating fair information practices. One could however question the viability of self-regulation by principles and codes because of the lack of efficient enforcement mechanisms to ensure the implementation and monitoring of database marketers' compliance with these. Current principles and codes of conduct are well formulated and have been adopted by several countries. It could therefore serve as a possible global guideline for protecting consumer privacy if the database marketing industry could find a way of enforcing the privacy principles.

A lack of efficient enforcement mechanisms is the major reason for failure of self-industry efforts to protect consumer privacy. At this point in time, industries have had only limited

success in implementing fair information practices and adopting self-regulatory programs with respect to the collection, use and dissemination of personal information. Industry commitment and enforcement mechanisms are essential components for the successful implementation of industry privacy principles. Current mechanisms used are administrative bodies, agencies or DMA's. However, these regulatory bodies do not hold much authoritative power and do not appear to be effective.

Another problem related to enforcement is the lack of legal redress to harmed individuals. Therefore, no punishment is given to deceptive and wrongful practices, so there is no need for complying with the codes and principles.

6.5.2.3 Typical advantages associated with industry self-regulation

Self-regulation is preferred to legislation efforts because the latter might restrict innovation and creativity within the database marketing industry. Self-regulation could therefore protect consumer privacy, without compromising innovation and creativity, which are essential elements in the marketing industry. Industry experts that understand the marketing practices and conditions could develop voluntary codes. Compliance to codes and principles tends to be better and enforced more readily, than would be the case with legislative control. Self-regulation should also be able to respond quicker than government intervention to changes in information technology that cause consumer privacy concerns. Lastly, industry self-regulation would be sufficient in regulating both online and traditional offline database marketing practices.

6.5.2.4 Possible role for the Direct Marketing Association of South Africa in self-regulation

Self-regulation efforts and a demonstration of concern for privacy must be communicated to society. Industry efforts should be clearly visible to public because this could alleviate consumers' concern for privacy. If consumers perceive the industry to care about privacy, it could alleviate privacy concerns. Industry efforts such as educational programs would promote consumer awareness. Consumers will therefore be more empowered to make informed choices on how to protect personal information. Consumers would also have more knowledge of possible trade-offs that exist between better product and service offerings, which resulted from having access to more consumer information.

The DMA of South Africa could monitor marketers' adherence to the Code of Practice by implementing periodic consumer and marketer reviews to ensure accurate databases. The DMA of South Africa should stress the need that proactive steps by marketers could alleviate consumer privacy concerns and reduce the need for legislation. Database marketing would not be able to develop to its full potential unless consumer confidence in the system is established. Hence, it makes business sense for industry to invest in self-regulation and consumer education.

6.5.3 Government intervention as means for regulating consumer privacy

Government intervention is another approach for protecting consumer privacy. Legislation, however, should be seen as the last resort for addressing the issue of consumer privacy. The arguments that support this statement will follow in the next paragraph. Database marketing practitioners would like to avoid regulation through privacy legislation. Government could however receive industry support if the industry was consulted or given the opportunity to make presentations in developing laws for regulating database marketing activities.

6.5.3.1 Typical problems associated with law enforcement

Advances and new developments in database technology continuously raise new consumer privacy concerns. The nature of government regulation of these database practices, on the other hand, changes very slowly. As a result, regulatory and legislative solutions to consumer protection are unlikely to be either timely or sufficiently flexible enough with respect to its information technology counterpart. Another argument against government intervention relates to the impact of legislation on regulating consumer privacy. The decentralised and global nature of database marketing will limit the effective monitoring of database marketing practices through legislation. Government would only have authorisation to regulate database marketing activities within a specific country and would not have authorisation to regulate cross-border flow of data. Therefore, one should rather consider other options, such as information technology that may provide more uniform protection on a global scale and that could regulate cross-border flow of consumer data. A further argument is that government intervention through the adoption of legislation, could pose restrictions on marketers' innovation and creativity. Legislation would most likely ignore the benefits and trade-offs provided by database marketing practices and would probably focus on protecting consumer privacy. Strict laws would restrict database marketing activities that invade consumer privacy

and would not necessarily consider the benefits consumers may receive if database marketers have access to consumer information. Another argument is that government intervention may infringe constitutional rights, as was the case with the Communication Decency Act of the United States of America. An individual's right to free speech could be threatened by laws that protect an individual's right to privacy. Therefore, most attempts to protect privacy restrict freedom of speech. Currently, the Constitution of the United States of America does not guarantee a right to privacy whereas it does guarantee a right to free speech. Government needs to consider the right to free speech when formulating policies for protecting consumer privacy.

6.5.3.2 The role of government in regulating consumer privacy

Government could enhance consumer privacy without imposing strict laws and regulations. Government should support industry efforts of self-regulation to ensure sustainable growth in database marketing. The greatest concern for self-regulation is the lack of an effective enforcement mechanism because this could mean that industry protection of consumer privacy may fail. Government should play a role in the implementation of principles. The implementation of principles can be promoted by the following:

- Encourage and support of self-regulation;
- Providing reasonable means for individuals to exercise the right to privacy;
- Providing of adequate remedies in case of failures to comply with industry codes and principles;
- Ensure that there is no unfair discrimination against data subjects;
- Adopting appropriate domestic legislation, as a last resort.

The mere fact that other alternatives to legislation are available, suggest that legislation, in conjunction with other means for protecting consumer privacy, should be considered. Government could assist in promoting consumer awareness through educational programs and could act as mediator between consumers and the industry. In South Africa, neither database marketing nor its impact on consumer privacy is well understood and therefore government and the public needs to be informed about database marketing practices. Government and the database marketing industry therefore have an important role in making consumers understand potential risks, as well as the trade-offs that accompanies the provision of

consumer information. However, consumer education is likely to raise demand for informational privacy protection.

Government should also encourage the development and implementation of information technologies that support consumer privacy. Parents could implement filtering software to protect children against harmful or unethical online database marketing practices.

Governmental control will be imposed if self-regulatory efforts and information technology fail to protect consumer privacy. Children, as a vulnerable group of consumers, would probably require law enforcement to ensure adequate protection of privacy.

6.6 A POSSIBLE MODEL FOR REGULATING DATABASE MARKETING PRACTICES IN SOUTH AFRICA

South Africa is in the unique position of having significant components that are typical of both developed and developing countries. The accepted international privacy principles were mainly developed from a first world perspective and one should take that into account when deciding upon possible policies and solutions for South Africa. This environment poses challenges that may differ from the developed world. Issues unique to South Africa should have a great influence when considering international practices for possible application in South Africa.

The next paragraph will consider Bennett's models for protecting consumer privacy and the Privacy Protection Model of Pincus and John. The appropriateness of these models for the South African environment will be evaluated considering relevant factors that may influence database marketing practices and the privacy concern of consumers.

6.6.1 Evaluating Bennett's models

Bennett's models are useful as departure points for existing measurements of global privacy protections. In this section an effort is made to identify, which model or combination of models are most appropriate for the conditions in South Africa.

6.6.1.1 The Voluntary Control Model

This model predominantly focuses on self-regulation efforts to protect consumer privacy. Therefore, the data gatherer is responsible for ensuring an adequate level of data protection. An independent individual must be appointed in order to ensure compliance to existing law. This model presumes that there exists some data protection law; the appointed individual is sufficiently independent; and enforcement will primarily rests on the aggrieved public. The United States of America implemented this model in combination with the Subject Control Model, but failed to provide adequate data protection. The Voluntary Control Model will most likely not succeed in South Africa. At present insufficient legislation as well as a lack of consumers awareness of privacy infringing data practices will hamper the working of this model. Consumers' privacy concerns are related to knowledge of invading data practices and South African consumers do not yet have high privacy concerns and consequently would not claim privacy rights. South Africans tend to be apathetic in nature and would unlikely claim such rights if consumers become aware of marketers' information practices. The absence of data protection laws will probably mean that data gatherers will not police themselves and the very core of the model would not function.

6.6.1.2 The Subject Control Model

This model requires participation and intervention by consumers to succeed. Again, consumers must be well informed of database marketing practices. Consumers should have the right to access data records and correct any inaccurate information. This model is not appropriate within the South African context. The typical South African consumer is relatively uninformed about data practices and is not assertive enough yet to claim privacy rights. South African consumers are uninformed due to inherent poor conditions for the majority of the society as well as non-educated communities. Database marketing practices have also yet to progress to an advanced level and therefore consumers are not aware of infringing data practices. The privacy concern of consumers in South African would probably increase when consumers become more knowledgeable about database marketing practices.

6.6.1.3 The Licensing Model

This model requires intervention by some governmental institution with regulatory and advisory powers to control the data collector and protect the relatively unskilled data subject.

The establishment of a higher level of privacy is possible with this model, but this model tends to have a bureaucratic approach. This model might have potential use in South Africa because consumers are uninformed and unskilled with regard to database marketing practices. Under this model an agency identifies conditions for data collection, use and dissemination and has regulatory powers to enforce compliance to such conditions. A benefit is the creation of data licences according to each data collector's needs. At present though, South African consumers do not have high privacy concerns compared to international privacy concerns, and this approach might be too strict. It has been argued that, preferably, government intervention should be the last option for protecting consumer privacy because it could impose restrictions on the free-market system. This model might therefore not be the only and best option for South Africa. The focus should rather be on an approach that addresses our level of privacy concern.

6.6.1.4 The Registration Model

The Registration Model is similar to the Licensing Model, except it does not involve an agency with regulatory powers but it acts like a notice system. An agency develops principles of fair information practices. Registration at this agency implies that marketers will adhere to the fair information privacy practices. Registered marketers would also be obliged to disclose data practices. The agency has no authoritative power to enforce compliance with these practices. The DMA of South Africa claims the industry provides means for consumers to opt out of company databases, but relatively few consumers have used this opportunity. This is a model that could be suitable for implementation in South Africa. The DMA of South Africa could act as the agency that develops fair information practices. The DMA of South Africa have already established a Code of Practices, to which database marketers needs to comply with. Since the privacy concern in South Africa is relatively low, this model would be useful for providing adequate data and consumer privacy protection. If consumer awareness of marketers' data practices increases, a greater need for privacy concern will likely result. The Registration Model could then be used in conjunction with another model such as the Data Commissioner Model, which will be discussed in the next section.

6.6.1.5 The Data Commissioner Model

A Data Commissioner has power to investigate complaints, constrain development of databases, review data practices and advise on improvements on data collectors' systems.

The Commissioner could also monitor advances in information technology that may enhance consumer privacy. This Commissioner has no authoritative power, but its success depends on good relationships with data collectors and education of the public so consumers could put pressure on those who do not comply with fair information practices. The models discussed earlier lack consideration of technology as a means for protecting privacy. Advancements in information technology should be monitored in order to ensure more effective protection and this is a requirement of the Data Commissioner Model. Furthermore, the DMA of South Africa could investigate complains and monitor compliance with fair information practices. The DMA of South Africa could also be held responsible for advising database marketing companies on improvements in data systems.

The Registration Model, together with elements of the Data Commissioner Model seem to be the appropriate models for protecting consumer privacy and for addressing privacy concerns in South Africa. This places the responsibility for data protection with the data collector or marketer, and the government. The Registration Model could act like a notice system where an agency, currently the DMA of South Africa develops principles of fair information practices to which registered marketers need to comply. A Commission, an element of the Data Commissioner Model, has power to investigate consumer complaints, constrain development of databases, review data practices and advise on improvements on data collectors' systems. The investigation and review of consumer complaints and database marketing practices could result in new policy formulation. The Commission could also monitor advancements in information technology that may enhance consumer privacy. It is important to incorporate information technology as a supplemental tool in regulating consumer privacy because it provides for the regulation of cross-border flow of consumer data. The continuous monitor of advances in information technology could therefore be useful in protecting consumer privacy. Neither industry self-regulation nor government intervention could regulate cross-border flow of data because of restrictions on authorised areas for regulation. This combination allows for industry self-regulation where registered members need to adhere to certain principles and codes of conduct. Industry self-regulation is important for ensuring that marketing innovation and creativity, which is essential to marketing practice, could flourish. The only problem seems to be that the agency and or the commission have no authoritative power to enforce compliance with principles and codes of conduct. One could argue though, that the privacy concern of South Africans are relatively low because consumers lack knowledge of database marketing practices. Therefore, the issue of lack of authoritative power to enforce compliance to principles are made less considerable.

These models could therefore be useful for providing adequate data and consumer privacy protection in South Africa.

6.6.2 Evaluating the Privacy Protection Model

This model is mainly concerned with determining a country's protection measures, relative to other countries protection measures. The model evaluates the level of data protection offered within different countries. This is accomplished by composing a privacy protection index, which includes the factors that needs to be evaluated to determine whether a country offers adequate protection, and a privacy protection scale, which plot countries on a continuum from no protection to complete protection. This model can be used to determine whether the specific Bennett's model employed in a country, is still efficient in providing adequate levels of privacy protection. Certain countries will differ with regard to the appropriate level of privacy protection. As consumers' attitudes and marketers' data practices change, the country's level of privacy protection needed, will change accordingly. However, the PPM must establish whether the employed model offers adequate privacy protection. If, for example a country such as the United States of America employed the Voluntary Control Model, the Privacy Protection Model would place them near the limited protection point on the privacy protection scale, because the Voluntary Control System in the United States of America failed to provide adequate levels of protection. Another one of Bennett's models could then be evaluated in terms of the Privacy Protection Model in order to determine whether adequate levels are provided by the implementation of that specific Bennett's model.

6.7 CONCLUSION

Bennett suggested several models for the protection of privacy. These include the Voluntary Control Model, the Subject Control Model, the Licensing Model, the Registration Model and finally the Data Commissioner Model. These models indicate which parties should be held responsible for monitoring and initiating the protection of privacy. Pincus and Johns proposed another model, namely the Privacy Protection Model. The value of this model lies in its qualitative nature. It measures a country's level of privacy protection in relation to other countries by plotting a country on a continuum with endpoints, no privacy and complete privacy. Bennett's models and Pincus and Johns's model could be useful in evaluating an appropriate system for protecting consumer privacy and for evaluating the effectiveness of such a system.

When formulating a policy for the protection of privacy the parties need to consider all the available means and approaches and also the different combinations thereof. The successful implementation of a protection policy in one country do not suggest that the same policy would be effective in another country because database marketing practices and consumer concerns in different countries vary to a great extend. Therefore, it is necessary to reconsider each and every factor that may have an influence on the development of an appropriate policy.

The Registration Model and the Data Commissioner Model seems a viable combination for implementation in South Africa because these models acknowledge the fact that South Africans are not well educated and informed enough on privacy invading database marketing practices. This combination does not involve any consumer participation, except for filing complaints. South African consumers are typical apathetic and as such it could be argued that South African consumers would prefer this option. The concern for privacy in South Africa has yet to progress to the level of consumers' concern in countries such as the United States of America and Europe. Industry self-regulation in conjunction with some governmental control and the application of information technology seems to be useful in providing adequate levels of privacy and data protection. Such a combination will hopefully strike a balance between South African consumers' need for privacy and South African marketers' need for consumer information.

6.8 SUGGESTIONS AND POSSIBLE OBJECTIVES FOR FUTURE RESEARCH

This study relied on literature and research projects from experts within the database marketing industry. The literature was however mainly concerned with database marketing practices and consumer privacy concerns within the United States of America and Europe. Few research projects have been done on the South African database marketing industry and the South African consumers' view thereof. More accurate conclusions and recommendations could be made after careful consideration and research on the South African database marketing industry.

Proposed research topics for the future could include the following:

- A comparison of database marketing activities and relevant privacy concerns between developing and developed countries;
- The influence of cross-cultural differences in regulating database marketing practice;

- A study on factors that threaten sustainable database marketing practices in South Africa;
- Examining the legal environment in which database marketers operate;
- Regulation of the South African database marketing industry;
- Factors that correlate with consumer privacy concern in South Africa;
- The impact of the Internet on the regulation of data practices and the protection of consumer privacy;
- Evaluating a model for protecting consumer privacy on a global scale.

These research topics firstly refer to database marketing within the South African environment. Research is necessary for objective consideration by policy makers. Secondly, the topics include the regulation of database marketing on a global scale. Globalisation and especially electronic means that enable global data collection and dissemination necessitates the establishment of some universal measure to protect consumers' information privacy. These issues need to be considered to ensure sustainable database marketing practices.

REFERENCES

Akdeniz, Y. (2000). New privacy concerns: ISP's, crime prevention and consumers' rights. International Review of Law, Computers & Technology, 14(1), 55-62.

Austin, M. J., & Reed, M. L. (1999). Targeting children online: Internet advertising ethics issues. Journal of Consumer Marketing, 16(6), 590-602.

Being traced over the Internet [online]. (2000). Available at: http://www.privacy.net/Traced/, 2000/12/18.

Berman, J., & Mulligan, D. (1999). Privacy in the digital age: Work in progress [online]. Available at: http://www.cdt.org.publications/lawreview/1999nova.shtml, 2000/12/18.

Birks, P. (Ed.). (1997). Privacy and loyalty. Oxford: Clarendon Press.

Bloom, P. N., Milne, G. R., & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations. Journal of Marketing, 58(1), 98-110.

Blosh, M. (1997). Information privacy: An annotated resource list. Prepared for the 1997 Spring Institute of the Northern California Association of Law Libraries [online]. Available at: http://www.nocall.org/privbib.html, 2000/12/18.

Briefly noted. (1997). Communication Abstracts, 20(6), 858.

Cavoukian, A. (1998). Privacy-enhancing technologies: Transforming the debate over identity. In C.J. Alexander & L.A. Pal (Eds.) Ditigal demogracy: Policy and politics in the wired world (181–193). Oxford: Oxford University Press.

Cespedes, F. V., & Smith, H. J. (1993). Database marketing: New rules for policy and practice. Sloan Management Review, 34(4), 7-22.

Consumer privacy concerns on the Internet [online]. (2000). Available at: http://hum142.tripod.com/ pond/cp.html, 2000/10/13.

Coyle, K. (1998). A primer on Internet privacy [online]. Available at: http://www.kcoyle.net/privacy primer.html, 2000/06/23.

Craig, J. R. (1998). Reno v. ACLU: The first amendment, electronic media, and the Internet indecency issue. Communications and the Law, 20(2), 1-14.

Cranor, L. F. (1996). The role of technology in self-regulatory privacy regimes [online]. Prepared for the National Telecommunications and Information Administration. Available at: http://www.research.att. com/~lorrie/pubs/NTIA.html, 2000/12/18.

Cranor, L. F. (1998). Internet privacy: A public concern [online]. Available at: http://www.research.att.com/~lorrie/publs/networker-privacy.html, 2000/06/23.

Cranor, L. F. (2000). Internet privacy and P3P: P3P working group chair [online]. Available at: http://www.research.att.com/projects/p3p/p3p-www9.ppt, 2000/06/23.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). Beyond concern: Understanding net users' attitudes about online privacy [online]. Available at: http://www.reasearch.att.com/ resources/trs/TRs/99/ 99.4/99.4.3/report.htm, 2000/06/23.

Culnan, M. J. (1993). How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly, 17(3), 341-361.

De Waal, J., Currie, I., & Erasmus, G. (1999). The Bill of Rights handbook (2nd ed.). Kenwyn: Juta.

Dempsey, J. X. (1997). Communications privacy in the digital age: revitalizing the federal wiretap laws to enhance privacy [online]. Available at: http://www.cdt.org/publications/ lawreview/1997albany.shtml, 2000/12/18.

Dentino, K. (1994). Taking privacy into our own hands. Direct Marketing, 57(5), 38-40, 42, 72.

The Direct Marketing Association [online]. (2000). Available at: http://www.pmg.org.za/ odb/Direct%20 Marketing%20Association.htm, 2000/11/08.

Direct Marketing Association of South Africa: Negative option marketing or inertia selling [online]. (2000). Available at: http://www.dma.org.za/Laws_stds/Inertia_selling.htm, 2000/12/18.

Direct Marketing Association of South Africa: About the DMA [online]. (2000). Available at: http://www.dma.org.za/about_the_dma.htm, 2000/12/18.

Direct Marketing Association of South Africa: DMA Code of Practice [online]. (2000). Available at: http://www.dma.org.za/Laws_stds/dma_code.htm, 2000/12/18.

Direct Marketing Association of South Africa: Frequently asked consumer questions about direct marketing [online]. (2000). Available at: http://www.dma.org.za/buy_direct_faq.htm, 2000/12/18.

Direct Marketing Association of South Africa: Glossary of direct marketing terminology [online]. (2000). Available at: http://www.dma.org.za/glossary.htm, 2000/12/18.

Direct Marketing Association of South Africa: On-line marketing principles [online]. (2000). Available at: http://www.dma.org.za/Laws_stds/online_marketing.htm, 2000/12/18.

Direct Marketing Association of South Africa: The consumer affairs committee consumer code for mail order marketing [online]. (2000). Available at: http://www.dma.org.za/Docs/Bpc_code.htm, 2000/12/18.

Direct Marketing Association of South Africa: The legal environment in which direct marketers operate. Promotion of access to information act [online link]. (2000). Available at: http://www.dma.org.za/ Laws_stds/laws.htm, 2000/12/18.

Direct Marketing Association of Southern Africa: Industry most frequently asked questions [online]. (2000). Available at: http://www.dma.org.za/industry_faq.htm, 2000/12/18.

Direct Marketing Association of Southern Africa: The privacy file [online link]. (1998). Available at: http://www.dma.org, 2000/12/18.

Effective enforcement of self-regulation [online]. (1998). Online Privacy Alliance. Available at: http://www.privacyalliance.org/resources/enforcement.shtml, 2000/09/29.

Electronic Privacy Information Center: The Code of Fair Information Practices [online]. (2000). Available at: http://www.epic.org/privacy/consumer/code_fair_info.html, 2000/12/18.

The end of privacy: The surveillance society. (1999, May). Economist, 351(8117), 15-20, 23.

Executive summary report: Proceedings to the industry Canada's symposium on privacy-enhancing technologies, Ottawa (1996, September 17). [online]. Available at: http://ecom.ic.gc.ca/english/privacy/ pv01167e.html#Pan1, 2000/05/04.

Federal Trade Commission's Staff Report (1996). Public workshop on consumer privacy on the global information infrastructure [online]. Available at: http://www.ftc.gov/reports/privacy/privacy1.htm, 1999/07/15.

Federal Trade Commission. (1998a, June). Privacy online: A report to congress (online). Available at: www.ftc.gov/reports/privacy3/priv-23a.pdf, 2000/12/16.

Federal Trade Commission. (1998b, July 21). Consumer privacy on the World Wide Web. Before the Subcommittee on telecommunications, trade and consumer protection of the house committee on commerce United States House of Representatives, Washington, D.C. [online]. Available at: http://techlawjournal.com/privacy/80721ftc.htm, 2000/12/16.

Federal Trade Commission. (2000). Privacy online: Fair information practices in the electronic marketplace: A report to Congress [online]. Available at: www.ftc.gov/os/2000/05/index.htm#22, 2000/10/24.

Flaherty, D. H. (1998). Visions of privacy: past, present, and future. 1996 Conference: "Visions of Privacy for the 21st Century. Available at http://www.oipcbc.org/publications/presentations/visions/html, 2000/10/24.

Flaherty, D. H. (1999). Computers and Privacy: How to regulate the private sector. Montreal International Conference on computers and law (online). Available at: http://www.law.warwick.ac.uk/ ltj/2-2k.html, 2000/10/24.

Froomkin, A. M. (1996). Flood control on the information ocean: Living with anonymity, digital cash, and distributed databases [online]. Available at: http://www.law.miami.edu/ ~froomkin/articles/ocean1. htm, 2000/11/09.

Groenewald, M. & Lehlokoe, D. (1999). Towards and electronic commerce policy for South Africa (online). Pretoria: Department of Communications, South Africa. Available at: http://www.isoc.org/ isoc/conferences/inet/99/proceedings/1g/1g-4.htm, 2000/12/18.

Grover, V., Hall, L., & Rosenberg, S. (1998). The web of privacy: Business in the information age. Business Horizons, 41(4), 5-11.

Hagel, J. (III), & Rayport, J. F. (1997). The coming battle for customer information. Harvard Business Review, 75(1), 53–55, 58, 60-61, 64-65.

Harvey, L. S. (2000). Information age changes marketing. National Underwriter/Life & Health Financial Services, 104(15), 31.

IP100 Plug-in: Proxemics [online]. (2000). Available at: http://www.stevelowe.co.nz/ip100/ manpi05.htm, 2000/10/13.

Kloesgen, W. (1995, April). Knowledge discovery in databases and data privacy. Proceedings of the IFEE Expert Symposium on knowledge discovery in databases vs personal privacy [online]. Available at: http://kdnuggets.com/gpspubs/ieee-expert-9504-priv.html., 2000/05/04.

Leonard, B. B. (1996, March 8). A primer on electronic data security. Published contribution to the Midwest Computer Conference '96 [online]. Available at: http://www.math.luc.edu/mcc96/papers/ leonard.html, 2000/05/04

Logsdon, T. (1980). Computers & social controversy. Potomac, Massachusetts: Computer science press.

Loro, L. (1998, October). Direct hits. Advertising Age's Business Marketing, 83(10), 17, 24.

Mainardi, J. (1997, February). Match the media to the message. Best's Review P/C, 97(10), 88-90.

McCroskey, J. C., Young, T. J., & Richmond, V. P. (2000). A simulation methodology for proxemic research [online]. Available at: http://www.as.wvu.edu/~jmccrosk/77.html, 2000/10/24.

McQuoid-Mason, D. (Ed.). (1997). Consumer law in South Africa. Kenwyn: Juta

Milne, G. R., Beckman, J., & Taubman, M. L. (1996). Consumer attitudes toward privacy and direct marketing in Argentina, Journal of Direct Marketing, 10(1), 22–33.

Moore, B. (Jr). (1984). Privacy: Studies in social and cultural history. Armonk, New York: M. E. Sharpe, Inc.

Morris, L., & Pharr, S. (1992, October). Invasion of privacy: A dilemma for marketing research and database technology. Journal of Systems Management, 10-11, 30-31, 42-42.

Mummert, H. (1997). Privacy ethics. Target Marketing, 20(5), 26-28.

Nowak, G. J., & Phelps, J. (1992). Understanding privacy concerns: An assessment of consumers' information-related knowledge and beliefs. Journal of Direct Marketing, 6(4), 28-39.

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. Journal of Direct Marketing, 9(3), 46-59.

O'Leary, D. E. (1995, April). Some privacy issues in knowledge discovery: OECD personal privacy guidelines. Proceedings of the IFEE Expert Symposium on knowledge discovery in databases vs personal privacy [online]. Available at: http://www/kdnuggets.com/gpspubs/ieee-expert-9504-priv.html, 2000/05/04.

OECD guidelines on the protection of privacy and transborder flows of personal data [online] (1980). Available at http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM, 2000/12/18.

Pallante, T. (1998). Distribution in the information age. Credit World, 86(5), 19–23.

Petrison, L. A., & Wang, P. (1995). Exploring the dimensions of consumer privacy: An analysis of coverage in British and American media. Journal of Direct Marketing, 9(4), 19–37.

Phelps, J., Gonzenbach, W., & Johnson, E. (1994). Press coverage and public perception of direct marketing and consumer privacy. Journal of Direct Marketing, 8(2), 9–22.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19(1), 27-52.

Piatetsky–Shapiro G. (1995, April). Guidelines for eating of the tree of knowledge, or knowledge discovery in databases vs. personal privacy. Proceeding of the IFEE Expert Symposium on knowledge discovery in databases vs personal privacy [online]. Available at: http://www/kdnuggets.com/gpspubs/ ieee-expert-9504-priv.html, 2000/05/04.

Pincus, L. B., & Johns, R. (1997). Private parts: A global analysis of privacy protection schemes and a proposed innovation for their comparative evaluation. Journal of Business Ethics, 16(12, 13), 1237–1260.

Privacy Inc's Consumer Privacy Guide. (1998). Available at: http://www.privacyinc.com, 2000/12/18.

The protection of privacy [online]. (2000). Available at: http://lsewww.epfl.ch/wilhelm/ thesis/node9. html, 2000/12/18.

Raab, C. D. (1997). Privacy, democracy, information. In B. D. Loader (Ed.). The governance of cyberspace (155-174). London: Routledge.

Rosenfield, J. R. (1996). Whither database marketing? Direct Marketing, 59(3), 40-41.

Saxby, S. (1990). The age of information. London: The Macmillan Press Ltd.

Selfridge, P. G. (1995, April). Privacy and knowledge discovery in databases. Proceedings of the IFEE Expert Symposium on knowledge discovery in datases vs personal privacy [online]. Available at: http://www/kdnuggets.com/gpspubs/ieee-expert-9504-priv.html, 2000/05/04.

Smith, R. M. (2000). Education: Web bugs FAQ [online]. Available at: http://www.privacy foundation.org/education.webbug.html, 2000/12/18.

Steer, D. (1999). Privacy practices help build trust, get and retain Web customers [online]. Available at: http://emcgt.com/Nov1999/feature.article.htm, 2000/12/18.

Taylor, R. E., Vassar, J. A., & Vaught, B. C. (1995). The beliefs of marketing professionals regarding consumer privacy. Journal of Direct Marketing, 9 (4), 38-46.

Valentine, D. (1999, Spring). About privacy: Protecting the consumer on the global information infrastructure. Proceedings to the Yale Symposium on law and technology [online]. Available at: http://lawtech.yale.edu/symposium/98/speech_valentine.htm, 2000/10/24.

Van den Haag, E. (1971). On privacy. In J.R. Pennock & J.W. Chapman (Eds.). Privacy. (pp. 149–168). New York: Atherton Press.

Varney, C. A. (1996, October). Consumer privacy in the information age: A view from the United States. Proceedings of the Privacy & American Business National Conference [online]. Washington DC. Available at: http://www.ftc.gov/speeches/varney/priv&ame.htm., 2000/10/24.

Weber, A. (2000). Building a customer value index [online]. Database Marketing Institute. Available at: http://www.dbmarketing.com/articles/art162.htm, 2000/12/18.

Westin, A. F. (1967). Privacy and freedom. New York: The Bodley Head Ltd.

What are haptics and proxemics? - Intercultural FAQ [online]. (2000). Available at: http://ic.intermundo.net/faq/heptics.shtml), 2000/10/13.

Ziarko, W. (1995, April). Response to O'Leary's article. Proceedings of the IFEE Expert Symposium on knowledge discovery in databases vs personal privacy [online]. Available at: http://www/kdnuggets.com/ gpspubs/ieee-expert-9504-priv.html, 2000/05/04.